ALGEBRO GEOMETRIC METHODS IN CODING THEORY

A DISSERTATION
SUBMITTED TO THE DEPARTMENT OF MATHEMATICS
AND THE INSTITUTE OF ENGINEERING AND SCIENCES
OF BILKENT UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
MASTER OF SCIENCE

By
İbrahim Özen
1999

ALGEBRO GEOMETRIC METHODS IN CODING THEORY

A DISSERTATION
SUBMITTED TO THE DEPARTMENT OF MATHEMATICS
AND THE INSTITUTE OF ENGINEERING AND SCIENCES
OF BILKENT UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
MASTER OF SCIENCE

By
İbrahim Özen
1999

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Prof. Dr. Alexander A. Klyachko(Principal Advisor)

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Prof. Dr. Hurşit Önsiper

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Prof. Dr. Serguei Stepanov

Approved for the Institute of Engineering and Sciences:

Prof. Dr. Mehmet Baray
Director of Institute of Engineering and Sciences

ABSTRACT

ALGEBRO GEOMETRIC METHODS IN CODING THEORY

İbrahim Özen
M.S. in Mathematics
Supervisor: Prof. Dr. Alexander A. Klyachko
1999

In this work, we studied a class of codes that, as a subspace, satisfy a certain condition for (semi)stability. We obtained the Poincaré polynomial of the nonsingular projective variety which is formed by the equivalence classes of such codes having coprime code length n and number of information symbols k. We gave a lower bound for the minimum distance parameter d of the semistable codes. We show that codes having transitive automorphism group or those corresponding to point configurations having irreducible automorphism group are (semi)stable. Also a mass formula for classes of stable codes with coprime n and k is obtained. For the asymptotic case, where n and k tend to infinity while their ratio $\frac{k}{n}$ is seperated both from 0 and 1, we show that all codes are stable.

Keywords: Linear code, variety, moduli sapce, stability, point configuration.

ÖZET

KODLAMA TEORİSİNDE CEBİRSEL GEOMETRİK METOTLAR

İbrahim Özen
Matematik Yüksek Lisans
Tez Yöneticisi: Prof. Dr. Alexander A. Klyachko
1999

Bu çalışmada alt uzay olarak (yarı)istikrarlılık sartını sağlayan kodlar incelendi. Kod uzunluğu n ve enformasyon sembol sayısı k'nın aralarında asal oldukları durumda bu kodların denklik sınıflarindan meydana gelen projektif varyetenin Poincaré polinomu elde edildi. Bu kodların minimum uzaklık parametresi d icin bir alt sınır belirlendi. Otomorfizma grubu gecişken olan veya indirgenemz otomorfizma grubu olan nokta konfigürasyonlarına karşılık gelen kodların (yarı)istikrarlı oldukları gösterildi. Aralarında asal n ve k'ya sahip kod denklik sınıfları için bir kütle formülü bulundu. Parametreleri n ve k'nın, oranları $\frac{k}{n}$'in 0 veya 1'den ayrı tutulmaları ve sonsuza yaklaşmaları durumunda bütün kodların (yarı)istikrarlı oldukları gösterildi.

Anahtar Kelimeler: Lineer kod, varyete, modüler uzay, istikrarlılık, nokta konfigürasyonu.

to **İsmail** and **İlhan**
to **my brothers**

ACKNOWLEDGMENT

Iwould like to express my gratitude to professor Klyachko for providing me his papers and necessary documents from which i learnt a lot and made use for this study. I also need to thank him for his excellent supervision and patience to my endless questions.

I owe the greatest of the thanks to my family who supported me all along my life. Nothing but their both moral and financial supports enlived my presence as a graduate student.

I want to thank to all my friends in Bilkent university. Hard times' friends Selim and Afif will be kept in my good memories of this era.

... and thank you Aysun for encouraging me to leave İstanbul.

Contents

Chapter 1

Introduction

1.1 Linear Codes

Due to the need of transfer of information in a healthy way, Information and Coding Theory has been a fast developing subject, bringing different branches of mathematics together since the study of Shannon [Sha] in 1948.

Linear codes appear to be an important means serving the objective of reliable information transfer *i.e.* the objective of transporting information in such a way that it is possible to recover the message from the received but possibly corrupted one. Detecting and correcting the errors which may occur while the transferring of the information is a part of the problem.

A linear code is a subspace C of a coordinate space $\mathbb{F}_q^n$ where $\mathbb{F}_q$ is a finite field of q elements. Information is carried by the vectors (code words) of C through the channel which is mostly noisy and distorting the code words. As we explain in chapter 2, if we take a code C with its dimension as a subspace k, each vector of C carries an information of k letters in its n symbols. We call k the number of information symbols and n the length of the code. At this point the question of how far we are away from the efficient use of time and energy is immediate. Efficiency in that sense is measured by the ratio $R = k/n$. From point of error correction, we pay attention to an other parameter of the code, that is the minimum number of nonzero places in nonzero code vectors of C. This parameter is called the minimum distance of the code and denoted by d. In this way we measure properties of codes by its parameters.

The multiplicative torus T^n has a natural action on vectors of $\mathbb{F}_q^n$ by coordinatewise multiplication. This action doesn't change the parameters of a code. Hence we call codes equivalent under action of T^n as equivalent codes.

The central problem of coding theory is algebraic construction of codes with given R and as large a d as possible.

1.2 Stable Codes

In our study we focus on a class of codes that are important in this respect.

Definition: A code $C \subset \mathbb{F}_q^n$ is said to be semistable if for any coordinate subspace $\mathbb{F}_q^I$ where

$$\mathbb{F}_q^I = \{(x_1, x_{2,}, \cdots, x_n) \in \mathbb{F}_q^n : x_j = 0 \ for \ j \notin I\} \quad I \subset [n]$$

the following inequalities hold

$$\frac{\dim(C \cap \mathbb{F}_q^I)}{|I|} \leq \frac{\dim C}{n}$$

and called stable if the inequalities are strict for $I \neq \emptyset, [n]$.

Example: The coordinate space $\mathbb{F}_q^n$ itself is semistable.

We use the term stable without consideration of the technical difference between semistable and stable in this discussion unless presicion is necessary. Since in the origin of coding theory are codes with good parameters, stable codes deserve a prior study. We can reduce the study of all codes to study of stable codes because once we are given a nonstable code C we can find a stable subcode $\tilde{C}$ with better parameters than those of C. We have shown this by the following proposition. (Proposition 2.5.)

Proposition: *For any nonstable code $C \subset \mathbb{F}_q^n$ there exists a (semi)stable code $\tilde{C}$ given by*

$$\tilde{C} := C \cap \mathbb{F}_q^I$$

where $\mathbb{F}_q^I$ is a destabilizing space with a minimal choice for I. Parameters of $\tilde{C}$ satisfy

$$\tilde{n} < n, \qquad \tilde{R} > R, \qquad \tilde{d} \geq d, \qquad \tilde{\delta} > \delta = \frac{d}{n}. \square$$

Beside what we have above we have the advantage of using machinery of algebraic geometry by studying stable codes. Codes with fixed length n and number of information symbols k are points on the Grassmannian $G(n,k)$. Stability in our definition is equivalent to Mumford stability of the subspace $C \subset \mathbb{F}_q^n$ w.r.t. the torus action on Grassmannian [Mum,Ch. IV, n.4]. As we learn from Geometric Invariant Theory [Mum] equivalence classes of semistable codes form a projective variety which we denote

$$\mathcal{C}_{n,k} = G(n,k)//T^n. \tag{1.1}$$

1.3 Stable Point Configurations

There is a one to one correspondance between orbits of diagonal torus $T^n \subset GL_n$ on subspaces of $\mathbb{F}_q^n$ which don't lie in a coordinate hyperplane and n point configurations in $\mathbb{P}^{k-1}$ modulo projective transformations. This correspondance is established by the so called Gelfand-MacPherson transformation

$$\varphi : G(n,k) \to \mathcal{C}_n(\mathbb{P}^{k-1}).$$

It is immediate from the definition that a stable code can not lie in a coordinate hyperplane. Gelfand-MacPherson transformation maps such a code C into a configuration of hyperplanes

$$C_i := C \cap \mathbb{F}_q^{[n]\setminus\{i\}}$$

cut out by the coordinate hyperplanes of $\mathbb{F}_q^n$. Furthermore we can pass to the dual space $\tilde{C}$ and take those lines σ_i vanishing on C_i's. The configuration $\Sigma(C) = \{\sigma_i\}_{i=1}^n$ is unique upto action of PGL_k.

Definition: A point configuration $\Sigma \subset \mathbb{P}^{k-1}$ is said to be semistable if the inequalities

$$\frac{|\Sigma \cap \mathbb{P}^{r-1}|}{r} \leq \frac{|\Sigma|}{k}$$

hold for $r \leq k$ and stable if the inequalities are strict for $r < k$.

Example: The configuration $\Sigma \subset \mathbb{P}^{k-1}$ of all rational points is semistable. Since

$$|\mathbb{P}^{i-1}(\mathbb{F}_q)| = \frac{q^i - 1}{q - 1},$$

we have

$$\frac{|\Sigma \cap \mathbb{P}^{r-1}|}{r} = \frac{q^r - 1}{(q-1)r} \leq \frac{q^k - 1}{(q-1)k} = \frac{|\Sigma|}{k}$$

by the monotonicity of the function

$$\frac{e^x - 1}{x} = \sum_{j \geq 0} \frac{x^j}{(j+1)!}$$

for positive x.

This definition is equivalent to Hilbert-Mumford stability of the point $\Sigma \in \mathbb{P}^{k-1} \times \mathbb{P}^{k-1} \times \ldots \times \mathbb{P}^{k-1}$ w.r.t action of PGL_k and Plücker embedding

$$(\mathbb{P}^{k-1})^n \hookrightarrow \mathbb{P}^N \qquad N = \binom{n}{k} - 1$$

[Mum, Ch. III, n.2].

Gelfand-MacPherson transformation carries stable codes to stable point configurations and even more establishes an isomorphism between the moduli space 1.1 and the invariant theoretical factor

$$\mathcal{C}_{n,k} = (\mathbb{P}^{k-1})^n // PGL_k.$$

For coprime n and k, this is a projective nonsingular variety of dimension $(k-1)(n-k-1)$.

1.4 The Main Result

The main result of this study is an explicit formula for the Poincaré polynomial

$$P_{n,k}(q) = \sum_s \beta_s q^s$$

of the moduli space $\mathcal{C}_{n,k}$ of stable n point configurations in $\mathbb{P}^{k-1}$ when $(n,k) = 1$ (Theorem 3.15).

It is immediate from the definition that for coprime n and k semistability of a code is equivalent to stability. In this case $\mathcal{C}_{n,k}$ is a projective nonsingular variety. Using combinatorial methods in [Kly] we calculate the number of rational points of this variety. It turns out that the number of rational points is given by a polynomial $P_{n,k}$ in q. Therefore $P_{n,k}(q)$ is the Poincaré polynomial

$$P_{n,k}(q) = \sum_s \beta_{2s} q^s \tag{1.2}$$

of $\mathcal{C}_{n,k}$ by Deligne-Weil theorem [Del] [Wei] *i.e.* coefficient β_{2r} of q^r is the $2r$th betti number of the variety $\mathcal{C}_{n,k}$. From code theoretical point of view it has an other significance. $P_{n,k}(q)$ is the number of stable codes with given length and number of information symbols over $\mathbb{F}_q$ upto equivalence when these two numbers are coprime. We give a list of examples for $P_{n,k}(q)$ in Appendix.

1.5 Applications

We give three applications of the above theory.

1.5.1 Codes with Big Automorphism Group

Codes with big automorphism group are especially interesting for coding theory. We have examined codes with transitive automorphism group and codes corresponding to configurations having irreducible group from point of stability. We give two theorems. (Theorems 2.13 and 2.14.)

Theorem: *Let C be a code with a transitive automorphism group, then C is semistable.* $\square$

Theorem: *Let Σ be a configuration of n points in $\mathbb{P}^{k-1}$ with irreducible automorphism group. Then the corresponding code $C(\Sigma) \in G(n,k)$ is semistable.* $\square$

Example: Cyclic codes are semistable.

We have a lower bound for the minimium distance parameter d of such codes by our following proposition. (Proposition 2.6.)

Proposition: *For a semistable code C the following inequality holds*

$$d(C) \geq \frac{1}{R(C)}.\square$$

1.5.2 Mass Formula for Stable Codes

Using Poincaré polynomial $P_{n,k}(q)$ we get a mass formula

$$M_{n,k}(q) = \sum_{class\ C} \frac{1}{|Aut(C)|} = \frac{P_{n,k}(q)}{n!}$$

for stable codes with given length and number of information symbols (Theorem 3.21). This formula counts equivalence classes of codes with a weight reciprocal cardinality of automorphism group of the class. In Appendix we give a table of masses of stable codes for a variety of choices n,k and q.

1.5.3 Asymptotic Behaviour of The Number of Stable Codes

In chapter 4, we investigate the asymptotic distribution of stable codes. When we consider codes with information rate R seperated both from 0 and 1 by a positive ϵ, we see that as n and k tend to infinity, ratio of the number of stable codes to the number of all codes tend to 1. Formally speaking, we prove the following theorem. (Theorem 4.1)

Theorem:

$$\lim_{n,k\to\infty} \frac{\#(stable[n,k]_q codes)}{\#(all[n,k]_q codes)} = 1$$

under the constraint

$$\epsilon < \frac{k}{n} < 1 - \epsilon \qquad\qquad 0 < \epsilon < 1.$$

Chapter 2

Preliminaries

2.1 Elements of Linear Codes

The basic concepts of linear codes are reminded and our notations are introduced in this section. We begin with definition of the very fundamental object, linear code.

Definition 2.1 A linear code is a subspace $C \subset \mathbb{F}^n$, where $\mathbb{F}$ is a finite field $\mathbb{F}_q$. Elements of C are called code vectors or code words.

2.1.1 Parameters of Linear Codes and Maximum Likelihood Decoding

Consider a k dimensional subspace $C \subset \mathbb{F}^n$. Once we fix a basis for C and form the $k \times n$ matrix G whose rows are the basis elements, we can generate the code C as an embedding of $\mathbb{F}^k$ into $\mathbb{F}^n$. Simply we multiply the elements of $\mathbb{F}^k$ on the right by G and get elements of C in $\mathbb{F}^n$. In this regard we call G a *generating matrix* of C.

Keeping in mind that C is outcome of this mapping we are in a position to send information of k letters by words of n digits in the transmission process.

We call k *the number of information symbols* and n *the length* of the code C. The class of codes over $\mathbb{F}_q$ with fixed length n and number of information symbols k, are called the $[n, k]_q$ codes.

One can discuss about the *rate* of this information transferring, which is denoted by $R = k/n$. Although it would be preferable to reduce the inefficiency, it is not always the case that we can achieve the most efficient coding by choosing $k = n$. In this case it wouldn't be possible to detect the possible defections of the code words during their transfer in the (noisy) channel.

We have so called *maximum likelihood decoding procedure* which enables us to detect such errors if we allow the redundant symbols in C to the price of inefficiency. An other important parameter is involved now. This parameter is defined via the Hamming distance

$$d : C \times C \longrightarrow \mathbb{Z}$$

which counts the number of places where two elements of $\mathbb{F}^n$ differ. We call minimum of those numbers for the pairs of different elements of C *the minimum distance* of C and denote it by d.

When we receive a vector we compare it with the code vectors. An error in the channel causes the code vectors change in some coordinates. If the number of such defected positions is less than d, then we will be aware that the received message is defected. Maximum likleihood decoding is to assign the defected vector the one that is closest in C. So that if we receive a vector which is not defected in more than $[\frac{d-1}{2}]$ places, we find the correct word that was transmitted. Together with d we have the *relative minimum distance* $\delta = d/n$ in the same normalization with R.

We find it convenient to mention here two fundamental problems of coding theory related with the parameters of codes. Shannon has proved that maximum transfer rate with neglicable errors is the capacity of the channel which depends on its physical characteristics. So that we can have codes with transfer rates R arbitrarily close to capacity of the channel. But all the proofs of this theorem is nonconstructive and one problem of coding theory is algebraic construction of such codes.

We have seen also that other than R there is one more important parameter δ for codes. For each code C, we have a point $P(C) = (\delta(C), R(C))$ in the unit square $[0,1]^2 \subset \mathbb{R}^2$. Mannin has shown that there is a continuous curve, dividing the square into two such that code points are dense in one part and isolated in the other. One of the fundamental problems of coding theory is learning about this curve, of which very little is known.

2.1.2 Automorphism Group of A Linear Code

One of the useful tools for understanding the nature of linear codes is the automorphism groups of codes. We consider the subgroup $\mathcal{G}$ of GL_n generated by transpositions of coordinates of elements in $\mathbb{F}^n$ and multiplying the i th coordinate by a nonzero scalar from $\mathbb{F}_q^*$. This group is represented by $n \times n$ matrices having one nonzero element in each row and each column. The automorphism group of a code C is the subgroup of $\mathcal{G}$ which fixes C as a subspace of $\mathbb{F}^n$.

Codes with big automorphism group turn out to be important, since those codes have big values of the parameter d.

2.2 Stable Codes and Stable Point Configurations

2.2.1 Stable Codes

The torus $T^n = \mathbb{F}_q^* \times \mathbb{F}_q^* \times \ldots \times \mathbb{F}_q^*$ has a natural coordinatewise action on the vector space $\mathbb{F}^n$. This action doesn't change the parameters of the codes, so calling the codes in the same orbit as equivalent codes makes sense.

Definition 2.2 A code $C \subset \mathbb{F}^n$ is said to be semistable if for any coordinate subspace $\mathbb{F}^I$ where

$$\mathbb{F}^I = \{(x_1, x_{2,}, \cdots, x_n) \in \mathbb{F}^n : x_j = 0 \; for \; j \notin I\} \quad I \subset [n]$$

the following inequalities hold

$$\frac{\dim(C \cap \mathbb{F}^I)}{|I|} \leq \frac{\dim C}{n} \tag{2.1}$$

and called stable if the inequalities are strict for $I \neq \emptyset, [n]$.

Remark: From the definition, it is clear that when $(n, k) = 1$ semistability implies stability.

Definition 2.2 is equivalent to stability of the subspace $C \subset \mathbb{F}^n$ w.r.t the torus action on Grassmannian $G(n, k)$ [Mum]. As we learn from the Geometric Invariant Theory [Mum] the equivalence classes of semistable subspaces form a projective variety

$$G(n, k)//T^n.$$

By the remark above, if n and k are coprime then semistability is equivalent to stability and in this case $G(n, k)//T^n$ is a projective *nonsingular* variety.

2.2.2 Gelfand-MacPherson Transformation and Stable Point Configurations

We can deal with the equivalence classes of semistable codes in geometric terms with the help of Gelfand-MacPherson transformation

$$\varphi : G(n, k) \to \mathcal{C}_n(\mathbb{P}^{k-1})$$

which maps a subspace $C \subset \mathbb{F}^n$ not lying in a coordinate hyperplane, to the configuration of hyperplanes in C cut out by the coordinate hyperplanes of $\mathbb{F}^n$. Correspondance between the hyperplanes and linear forms helps us map the code into a configuration of points in the dual projective space $\widehat{\mathbb{P}}^{k-1}$. This configuration is considered up to linear transformations of C and gives a one to one correspondance between the orbits of T^n on $G(n, k)$ (when it is well defined) and configurations of n points in $\mathbb{P}^{k-1}$ with trivial intersection modulo projective transformations. We call such a configuration $\Sigma \subset \mathbb{P}^{k-1}$ a *constellation*. Coordinates of points $p \in \Sigma$ can be choosen to form the columns of the generating matrix of the corresponding code $C = C(\Sigma)$ as pointed out in [T-V]. Code parameters after the transformation takes the form

$$\begin{aligned} |\Sigma| &= \text{code length} \\ k &= \text{number of information symbols} \\ \min_{\mathbb{A}^{k-1} \subset \mathbb{P}^{k-1}} |\Sigma \cap \mathbb{A}^{k-1}| &= \text{minimum distance} \end{aligned}$$

Where min is taken over all affine planes $\mathbb{A}^{k-1} \subset \mathbb{P}^{k-1}$.

We'll see that the moduli space $G(n,k)//T^n$ is mapped to an other moduli space by Gelfand-MacPherson transformation.

Definition 2.3 A point configuration $\Sigma \subset \mathbb{P}^{k-1}$ is said to be semistable if the inequalities

$$\frac{|\Sigma \cap \mathbb{P}^{r-1}|}{r} \leq \frac{|\Sigma|}{k} \tag{2.2}$$

hold for $r \leq k$ and stable if the inequalities are strict for $r < k$.

This definition is equivalent to Hilbert-Mumford stability of the point $\Sigma \in \mathbb{P}^{k-1} \times \mathbb{P}^{k-1} \times \ldots \times \mathbb{P}^{k-1}$ w.r.t action of PGL_k and Plücker embedding [Mum]

$$(\mathbb{P}^{k-1})^n \hookrightarrow \mathbb{P}^N \qquad N = \binom{n}{k} - 1.$$

Proposition 2.4 *Gelfand-MacPherson transformation maps a (semi)stable code $C \subset \mathbb{F}^n$ into a (semi)stable configuration $\Sigma \in (\mathbb{P}^{k-1})^n$ and induces an isomorphism of invariant theoretical factors*

$$\varphi : G(n,k)//T^n \to (\mathbb{P}^{k-1})^n//PGL_k.$$

Proof: First we show that Gelfand-MacPherson transformation carries stability condition in 2.1 to the one in 2.2. Consider a coordinate subspace $\mathbb{F}^I$ $I \subset [n]$. Let

$$J = [n] \setminus I$$

If we denote the hyperplane in C cut out by the coordinate hyperplane having the jth place is zero by C_j we have the equality

$$\dim(C \cap \mathbb{F}^I) = \dim(C_{j_1} \cap C_{j_2} \cap \ldots \cap C_{j_m})$$

where j_i run in J. As we discussed above those hyperplanes C_{j_i} are mapped to lines p_{j_i} in the dual space of C. Hence we have

$$k - \dim(\mathrm{span}\{\mathrm{p}_{\mathrm{j}_1}, \mathrm{p}_{\mathrm{j}_2}, \ldots, \mathrm{p}_{\mathrm{j}_m}\}) = \dim(\mathrm{C}_{\mathrm{j}_1} \cap \mathrm{C}_{\mathrm{j}_2} \cap \ldots \cap \mathrm{C}_{\mathrm{j}_m})$$

The inequality 2.1 is transformed into

$$\begin{aligned}\frac{k-\dim(\mathrm{span}\{\mathrm{p_j}\}_{\mathrm{j}\in\mathrm{J}})}{n-|J|} &\leq \frac{k}{n}\\ \frac{|J|}{\dim(\mathrm{span}\{\mathrm{p_j}\}_{\mathrm{j}\in\mathrm{J}})} &\leq \frac{n}{k}\end{aligned}$$

Remembering that the configuration corresponding to a code which doesn't lie in a coordinate hyperplane spans the space, the last form of the inequality is what we want to get. It is clear that the transformation is one-one. □

2.3 Parameters of Stable Codes

In this subsection we clarify why study of stable codes is important. We can construct a stable code out of a nonstable one and in the end we have a code with better parameters. Moreover we have a lower bound for the minimum distance of a semistable code.

Proposition 2.5 *For any nonstable code $C \subset \mathbb{F}^n$ there exists a (semi)stable code $\tilde{C}$ with parameters*

$$\tilde{n} < n, \qquad \tilde{R} > R, \qquad \tilde{\delta} > \delta, \qquad \tilde{d} \geq d.$$

Proof: Let $\mathbb{F}^I \subset \mathbb{F}^n$ be a destabilizing subspace for which

$$\frac{\dim(C \cap \mathbb{F}^I)}{|I|} > \frac{\dim(C)}{n} = R$$

holds and let

$$\tilde{C} := C \cap \mathbb{F}^I \subset \mathbb{F}^I$$

be the code with

$$\tilde{n} = |I| < n.$$

$\tilde{C}$ has transfer rate

$$\tilde{R} = \frac{dim(C \cap \mathbb{F}^I)}{|I|} > \frac{k}{n} = R.$$

Since $\tilde{C} \subset C$ then $\tilde{d} \geq d$ and hence

$$\tilde{\delta} > \delta$$

is clear. If we choose in the construction above $\mathbb{F}^I$ with a minimal $I \subset [n]$ stability of $\tilde{C}$ is easily seen. □

Proposition 2.6 *A semistable code $C = C(\Sigma)$ satisfies*

$$d \geq \frac{1}{R}.$$

Proof: The semistable code C corresponds to the semistable configuration Σ. We know by 2.2 that

$$|\Sigma \cap \mathbb{P}^{k-2}| \leq \frac{(k-1)n}{k}.$$

If we substitute this and estimate, we get

$$d = \min_{\mathbb{A}^{k-1} \subset \mathbb{P}^{k-1}} |\Sigma \cap \mathbb{A}^{k-1}| = n - \max_{\mathbb{P}^{k-2} \subset \mathbb{P}^{k-1}} |\Sigma \cap \mathbb{P}^{k-2}| \geq n - \frac{(k-1)n}{k} = \frac{n}{k} = \frac{1}{R}. \square$$

2.4 Canonical Filtration of a Configuration

We introduce the main tool of the study in this section. The whole section is exposition of the ideas in [Kly1]. We'll show that stability of a configuration (or of the corresponding code) can be checked via its canonical filtration. Since we are dealing with point configurations in a projective space, we find the equivalent study of line configurations in a vector space more convenient for simplicity.

Now we define a characteristic class of a configuration Σ of 1 dimensional subspaces of a vector space V

$$c(V) = |\Sigma \cap V|.$$

By means of $c(V)$ we define the slope of the configuration as

$$\mu(V) = \frac{c(V)}{\dim V}.$$

We can reword the definition 2.3 for 1-spaces in a linear space V.

Definition 2.7 A configuration Σ of 1-spaces in V is semistable if

$$\mu(U) \leq \mu(V)$$

for any subspace $U \subset V$ with the induced configuration

$$U_\Sigma = U \cap \Sigma,$$

and we say that the configuration is stable if the inequalities are strict for $U \neq 0, V$.

Let's fix our space V and configuration Σ.

Proposition 2.8 *For any pair of subspaces $F, G \subset V$ with induced configurations, the following inequality holds*

$$c(F \cap G) + c(F + G) \geq c(F) + c(G) \tag{2.3}$$

Proof: Let $\sigma \in \Sigma$ be a line in the configuration. We have

$$(F + G)_\sigma \supset F_\sigma + G_\sigma$$

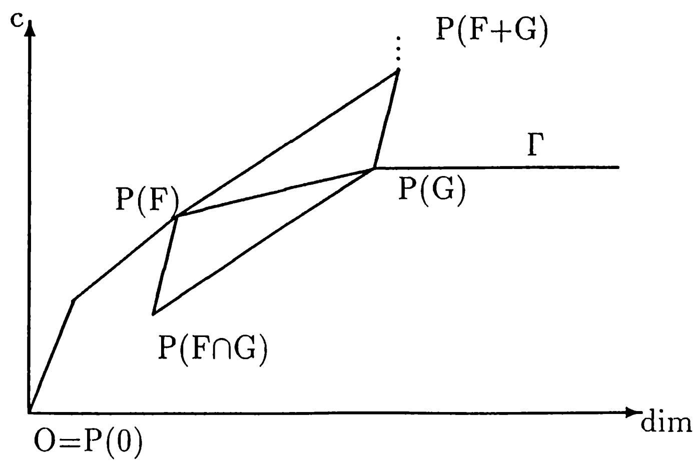
hence,

$$\begin{aligned} \dim(F + G)_\sigma &\geq \dim(F_\sigma + G_\sigma) \\ \dim(F \cap G)_\sigma + \dim(F + G)_\sigma &\geq \dim F_\sigma + \dim G_\sigma \end{aligned}$$

Summation over $\sigma \in \Sigma$ gives the desired result.$\Box$

Now we make comments on geometric interpretation of the proposition. Let's represent a subspace $F \subset V$ by a point $P(F) = (\dim(F), c(F))$ on the plane $\mathbb{R}^2$.

If we draw a parallelogram three vertices determined by $P(F), P(G)$ and $P(F + G)$, then by the proposition above, the fourth vertice opposite to $P(F + G)$ lies below the point $P(F \cap G)$. Or, $P(F)$ is lower than the vertex opposite to $P(G)$ in the parallelogram whose three vertices are determined by the points $P(F + G), P(F \cap G)$ and $P(G)$.



Now let's consider a convex hull of all points $P(F)$ for subspaces $F \subset V$. Its upper boundary is a polygonal line Γ connecting the points $O = P(0)$ and $P(V)$.

Proposition 2.9 *There exists a unique subspace $F_\nu \subset V$ that corresponds to a vertex ν of Γ. These subspaces form a chain.*

Proof: We begin with the second statement. Let subspaces $F, G \subset V$ correspond to the adjacent vertices of the polygonal line Γ. Then all points $P(H), H \subset V$, lie either on the segment $[P(F), P(G)]$ or below the line passing through these two points. But the proposition 2.8 implies that the point $P(F+G)$ lies above the vertex opposite to $P(F \cap G)$ of the parallelogram constructed by the three points $P(F), P(G)$ and $P(F \cap G)$. Hence the point $P(F+G)$ corresponds either to $P(F)$ or to $P(G)$ (one that lies farther to right) say $P(G)$, then

$$\begin{aligned} \dim(F+G) &= \dim G \\ F &\subset G \end{aligned}$$

Applying the same idea, the parallelogram degenerates to a line segment in the case of unicity of the space, hence we have the result.□

We proved that, to a configuration Σ there corresponds a unique chain of subspaces in V, forming an upper convex polygonal line when represented in the plane $\mathbb{R}^2$ as described above.

Definition 2.10 The chain of subspaces $F_\nu \subset V$ of proposition 2.9 ν a vertex of Γ, is called the canonical filtration of the configuration Σ of 1-spaces in V.

Now we give a characterization of the canonical filtration.

Proposition 2.11 *Let V and Σ be given. Suppose that the induced configurations on composition factors $F_{[i]} = F_i/F_{i-1}$ of a filtration*

$$\mathcal{F} : 0 = F_0 \subset F_1 \subset \ldots \subset F_m = V$$

are semistable and their slopes are strictly decreasing

$$\mu(F_{[i]}) > \mu(F_{[i+1]}). \tag{2.4}$$

Then $\mathcal{F}$ is the canonical filtration of the configuration Σ.

Proof: Let $\Gamma(\mathcal{F})$ be the polygonal line with vertices $P(F_i)$. Condition 2.4 implies that the successive line segments $[P(F_i), P(F_{i+1})]$ have decreasing slopes, hence Γ is upperconvex.

We are given that the induced configuration in composition factor $F_{[i]}$ is semistable on that space. This condition makes sure that for any U, $F_{i-1} \subset U \subset F_i$, the point $P(U)$ lies below the diagonal $[P(F_{i-1}), P(F_i)]$ of the rectangle formed by these two opposite vertices. We can use this idea to show that for any subspace $U \subset F_i$, the point $P(U + F_{i-1})$ lies below Γ ($F_{i-1} \subset U + F_{i-1} \subset F_i$). We prove by induction on i that for any subspace $E \subset Fi$, the corresponding point $P(E)$ lies below Γ. By induction hypothesis $P(E \cap F_{i-1})$ is below Γ. One more use of the proposition 2.8 will show us that the point $P(E)$ lies below the vertex opposite to $P(F_{i-1})$ in the parallelogram constructed by the vertices $P(F_{i-1}), P(E \cap F_{i-1})$ and $P(E + F_{i-1})$. Hence we proved $P(E)$ lies below $\Gamma(\mathcal{F})$ for any $E \subset V$. □

Theorem 2.12 *A configuration Σ of 1-spaces in V is semistable if and only if its canonical filtration is trivial.*

Proof: Definition of canonical filtration and the previous proposition leaves no need for any proof.□

Theorem 2.13 *Let C be a code with transitive automorphism group. Then C is semistable.*

Proof: Since C has transitive automorphism group, it can not lie in a coordinate hyperplane (unless it is trivial), hence Gelfand-MacPherson transformation is well defined and we can consider the dual point configuration Σ corresponding to C.

Automorphism group fixes the canonical filtration $\mathcal{F}_\Sigma$ (from uniqueness of c.f. and proposition 2.11) as well as Σ . Let

$$\sigma_i \in F_j \qquad \sigma_i \in \Sigma \textit{ and } F_j \in \mathcal{F}_\Sigma$$

Since σ_i is equivalent to all σ_k's and F_j is fixed by the automorphism group, then F_j contains all the elements in Σ . But Σ spans the space (columns of the genrating matrix), hence $F_j = \hat{C}$. Canonical filtration is trivial and we get the result. □

Theorem 2.14 *Let Σ be a configuration of lines in a vector space V with irreducible automorphism group $\mathcal{A} \subset PGL(V)$. Then Σ is semistable.*

Proof: Let

$$\mathcal{F} : F_0 \subset F_1 \ldots \subset F_m = V$$

be the canonical filtration of Σ. Since $\mathcal{F}$ has to be fixed by $\mathcal{A}$ and $\mathcal{A}$ is irreducible, there is no $F_j \in \mathcal{F}$ with $F_j \neq 0, V$. Canonical filtration is trivial and Σ is semistable. □

Theorem 2.15 *The minimum distance parameter d of cyclic codes satisfies*

$$d \geq \frac{1}{R}.$$

Proof: This is a direct consequence of the proposition 2.6 and theorem 2.13. □

Chapter 3

Poincaré Polynomial of $\mathcal{C}_{n,k}$ when $(n,k) = 1$

In this chapter we evaluate the Poincaré polynomial

$$P_{\mathcal{C}_{n,k}}(x) = \sum_i \beta_i x^i$$

of the variety $\mathcal{C}_{n,k}$ for coprime n and k. The coefficient β_j is the jth Betti number of $\mathcal{C}_{n,k}$.We make use of the combinatoric methods in [Kly1] to achieve this goal.

When $(n,k) = 1$, $\mathcal{C}_{n,k}$ is a projective nonsingular variety. We find the number of rational points this variety over $\mathbb{F}_q$. It turns out that the number of rational points is given by a polynomial $P_{n,k}$ in q. By Deligne-Weil [Del] [Wei] theorem we conclude that $P_{n,k}(q)$ is the Poincaré polynomial

$$P_{n,k}(q) = \sum_i \beta_{2i} q^i,$$

of $\mathcal{C}_{n,k}$.

In the following discussion, we denote the number of ordered n line configurations in a k dimensional vector space over $\mathbb{F}_q$ by $R_q(n,k)$. Canonical filtrations of the configurations will help us find a recurrence relation for $R_q(n,k)$. We solve this recurrence relation by introducing the notion of *hierarchy* for decompositions of the pair (n,k) as in

$$
\begin{aligned}
(n,k) &= ((n_1,k_1),(n_2,k_2),\ldots,(n_m,k_m)) \qquad \textit{where} \\
n &= n_1+n_2+\ldots+n_m \\
k &= k_1+k_2+\ldots+k_m.
\end{aligned}
$$

At this point we get $R_q(n,k)$ as a sum taken over normalized hierarchies whose terms are quite simple except for a coefficient a. We find the coeefficient a by help of Combinatoric Geometry of the Plane. In the end $R_q(n,k)$ is a polynomial given by a sum taken over decompositions of (n,k) which satisfy

$$\frac{n_i}{k_i} > \frac{n}{k}.$$

Stable line configurations have no pointwise automorphisms, hence we find that the number of rational points of $\mathcal{C}_{n,k}$ is given by

$$P_{n,k}(q) = \frac{R_q(n,k)}{|PGL_k|}.$$

It should be kept in mind that we deal only with the case $(n,k)=1$ in the following sections.

3.1 Recurrence Relation for $R_q(n,k)$

To begin with, we choose to find the number of lines having given projection on the filtration

$$\mathcal{F} : F_0 \subset F_1 \subset \ldots \subset F_m = V.$$

Proposition 3.1 *Let k_i denote the dimension of the composition factor $F_{[i]}$ of the filtration*

$$\mathcal{F} : F_0 \subset F_1 \subset \ldots \subset F_m = V$$

and let n_i be the number of lines fixed in the same factor. Then the number of lines in V having projections those fixed lines in the filtration $\mathcal{F}$ is given by

$$q^{\sum_{i<j} k_i n_j}.$$

Proof: Let's fix a configuration Σ of lines and let $\sigma \in \Sigma$ lying in $F_{[i]} = F_i/F_{i-1}$. The vectors in V whose projection on $F_{[i]}$ is parallel to σ form a linear space of dimension $\dim F_{i-1}$. So there are $q^{\dim F_{i-1}}$lines having given projection σ for each $\sigma \in \Sigma$. If the number of lines in $F_{[i]}$ of Σ is given by n_i then we have a total of $q^{n_i \dim F_{i-1}}$ lines in V with given projection. □

Now we introduce the notations which will be used heavily in the following discussion. Those are Gaussian multinomial coefficients.

$$[k]_q = \frac{q^k - 1}{q - 1}. \tag{3.1}$$

$$[k]_q! = [k]_q[k-1]_q[k-2]_q \dots [1]_q. \tag{3.2}$$

$$\begin{bmatrix} k \\ k_1 k_2 \dots k_m \end{bmatrix}_q = \frac{[k]_q!}{[k_1]_q![k_2]_q! \dots [k_m]_q!}. \tag{3.3}$$

Proposition 3.2 *Let $k_1, k_2, \dots, k_m$ be a sequence of dimensions of composition factors of a filtration in V. The number of such filtrations is*

$$\begin{bmatrix} k \\ k_1 k_2 \dots k_m \end{bmatrix}_q . \square$$

In the previous chapter, we have seen that every configuration of n lines in V has a unique canonical filtration(Proposition 2.9). Also it is worth reminding that intersection of the configuration with the composition factors of its canonical filtration is semistable in that factor space. This relation enables us to determine the number of all configurations in terms of the canonical filtrations and the number of semistable configurations of given n and k.

We begin with grouping configurations according to their canonical filtrations.

$\#$(n line conf. in V)=$\sum_{\mathcal{F}}\#$(n line conf.s with canonical filtration $\mathcal{F}$) (3.4)

If we fix the dimensions of composition factors of the canonical filtrations by k_i's and the numbers of lines contained in those factor spaces by n_i's we can put equation 3.4 in a more formal language. In the following discussion $R_q(n, k)$ denotes the number of semistable configurations of n lines in a k dimensional vector space.

Theorem 3.3

$$[k]_q^n = \sum_{\substack{n_1+n_2+\ldots+n_m=n \\ k_1+k_2+\ldots+k_m=k \\ \frac{n_1}{k_1}>\frac{n_2}{k_2}>\ldots>\frac{n_m}{k_m}}} \begin{bmatrix} k \\ k_1 k_2 \ldots k_m \end{bmatrix}_q \begin{pmatrix} n \\ n_1 n_2 \ldots n_m \end{pmatrix} q^{\sum_{i<j} k_i n_j} \prod_i R_q(n_i, k_i)$$

Proof: Left hand side is the number of all n line configurations in a k dimensional space. On the right hand side, we take sum over all canonical filtrations. We fix the canonical filtrations with the dimensions of their composition factors and the preassigned number of semistable line configurations lying on those compositions. The Gaussian multinomial coefficient counts the number of filtrations with given dimensions of composition factors. We construct a total of n lines by taking n_i from each composition factor of dimension k_i. The product of $R_q(n_i, k_i)$'s determines the number of possible constructions. However in the space V we have $q^{\sum_{i<j} k_i n_j}$ configurations with given projections on the composition factors. And we count the possible rearrangements of n elements where the orderings of n_i elements were already included in the term $R_q(n_i, k_i)$ by the binomial coefficients.□

We know by theorem 2.12 of the previous chapter that, the semistable configurations have trivial canonical filtrations. Hence we can extract $R_q(n, k)$ from the theorem above

$$R_q(n,k) = [k]_q^n - \sum_{\substack{n_1+n_2+\ldots+n_m=n \\ k_1+k_2+\ldots+k_m=k \\ \frac{n_1}{k_1}>\frac{n_2}{k_2}>\ldots>\frac{n_m}{k_m}}} \begin{bmatrix} k \\ k_1 k_2 \ldots k_m \end{bmatrix}_q \begin{pmatrix} n \\ n_1 n_2 \ldots n_m \end{pmatrix} q^{\sum_{i<j} k_i n_j} \prod_i R_q(n_i, k_i) \quad (3.5)$$

where now the sum is taken over all nontrivial canonical filtrations.

What we have at the moment is a recurrence relation. For an explicit formula, we have to apply this to all pairs (n_i, k_i) and to their decompositions and so on.

At this point we begin changing our notations. Having given the necessary motivations and explanations about the decompositions of n and k with condition $n_i/k_i > n_{i+1}/k_{i+1}$, from now on we will denote the index of our sum with decompositions of the pair (n, k). Let's call the pairs *cells* and the ratio n/k *slope* of the cell. So our formula will be denoted

$$R_q(n,k) = [k]_q^n - \sum_{(n_1,k_1)(n_2,k_2)\ldots(n_m,k_m)} \begin{bmatrix} k \\ k_1 k_2 \ldots k_m \end{bmatrix}_q \begin{pmatrix} n \\ n_1 n_2 \ldots n_m \end{pmatrix} q^{\sum_{i<j} k_i n_j} \prod_i R_q(n_i, k_i)$$

where the sum is taken over nontrivial decompositions of the cell (n, k) into smaller cells with their slopes strictly decreasing from left to right.

3.2 Normalized Hierarchies

The notion of a cell is still far from being enough to carry the successive applications of our formula. Hence we continue developing our notations and introduce the so called *hierarchy.*

Definition 3.4 A hierarchy J is a decomposition of the pair (n, k) into cells *with levels.*

The cell (n, k) itself is the only cell of level 0. We decompose (n, k) in a nontrivial way and call new cells as *cells of level 1.* And we continue the process, dividing some of cells of level 1 into cells of level 2, and some of them into cells of level 3. We can stop at any step and call this decomposition a hierarchy. The cells that we stop decomposing are called *atoms* of the hierarchy. We denote hierarchies with bracket structures. For example

$$((n_1, k_1), \ldots, (n_4, k_4))_J = ((n_1, k_1), ((n_2, k_2), (n_3, k_3)), (n_4, k_4)).$$

Each pair in a balanced pair of brackets denote a cell. We don't use double brackets. Our sample hierarchy contains

$$\begin{array}{rl} (n_1, k_1), (n_2 + n_3, k_2 + k_3), (n_4, k_4) & \text{cells of level 1,} \\ (n_2, k_2), (n_3, k_3) & \text{cells of level 2,} \\ (n_1, k_1), \ldots, (n_4, k_4) & \text{atoms.} \end{array}$$

Keeping in mind the motivation of defining hierarchies, we have to put a normalization condition on our hierarchies.

Definition 3.5 A hierarchy J is said to be normalized if for any cell

$$(n, k) = ((n_1, k_1), (n_2, k_2), \ldots, (n_m, k_m))$$

the slopes of the cells (n_i, k_i) of the next level decrease from left to right.

$$\frac{n_i}{k_i} > \frac{n_{i+1}}{k_{i+1}} \tag{3.6}$$

Definition 3.6 We denote by $NA(J)$ the number of nonatom cells in the hierarchy J. The number $(-1)^{NA(J)}$ is called the sign of J.

In the preceding notations, the formula in equation 3.5 can be given as

Proposition 3.7

$$R_q(n,k) = \sum_{((n_1,k_1)(n_2,k_2)\dots(n_m,k_m))_J} (-1)^{NA(J)} \left[\begin{array}{c} k \\ k_1 k_2 \dots k_m \end{array} \right]_q \left(\begin{array}{c} n \\ n_1 n_2 \dots n_m \end{array} \right) q^{\sum_{i<j} k_i n_j} \prod_i [k_i]_q^{n_i}$$

The summation is conducted over all normalized hierarchies.

Proof: The foregoing explanations leave no need for any further proof.□

We see that the new form of our formula depends mostly on the set of atoms of the hierarchies. If we fix the set of atoms and define a new coefficient

$$a((n_1,k_1),(n_2,k_2),\dots,(n_m,k_m)) = \sum_{atoms:(n_1,k_1),(n_2,k_2),\dots,(n_m,k_m)\ J} signJ \quad (3.7)$$

our formula takes the form

$$R_q(n,k) = \sum_{(n_1,k_1)(n_2,k_2)\dots(n_m,k_m)} a((n_1,k_1),\dots,(n_m,k_m)) \left[\begin{array}{c} k \\ k_1 k_2 \dots k_m \end{array} \right]_q \left(\begin{array}{c} n \\ n_1 n_2 \dots n_m \end{array} \right) q^{\sum_{i<j} k_i n_j} \prod_i [k_i]_q^{n_i} (3.8)$$

3.3 Combinatorial Geometry of the Plane

Now we will discuss the geometric interpretation of the normalization condition and the coefficient a defined in 3.7. For easiness in notation we denote an atom (n_i,k_i) by Λ_i. We represent a cell $\Delta = (n_r,k_r)$ by a point $P(\Delta) = (k_r,n_r)$ on the plane $\mathbb{R}^2$. Suppose we deompose $\Lambda = (n,k)$ as in $\Lambda = (\Lambda_1,\Lambda_2,\dots,\Lambda_m)$. This decomposition will be represented by a polygonal line $\Gamma(\Lambda_1,\Lambda_2,\dots,\Lambda_m)$, with consequtive vertices $\nu_i = P(\Lambda_{\leq i})$, $\Lambda_{\leq i} = (\sum_{j=1}^{i} n_j, \sum_{j=1}^{i} k_j)$ for $0 \leq i \leq m$ and $\nu_0 = (0,0)$.

Let's apply this to a normalized hierarchy J. We consider the first level decomposition

$$\Lambda = (\Delta_1,\Delta_2,\dots,\Delta_r).$$

We keep our notations and denote the slope of a cell Δ by $\mu(\Delta)$.The normalization condition 3.6 assures that

$$\mu(\Delta_i) > \mu(\Delta_{i+1}).$$

This results an upper convex polygonal line Γ^1 when we join the successive vertices ν_i as described above.

In the same way, we can take the first level cell Δ_i and decompose it into cells of level 2 as in $\Delta_i = (\Delta_{i1}, \Delta_{i2}, \ldots, \Delta_{ir_i})$. In the plane, process goes on by putting the point $P(\Delta_1, \Delta_2, \ldots, \Delta_{i-1}, \Delta_{i1}) = (k_{\leq i-1} + k_{i1}, n_{\leq i-1} + n_{i1})$ and joining it to $P(\Delta_{i-1})$. We complete Γ_i^2 beginning at $P(\Delta_{\leq i-1})$ and ending at $P(\Delta_{\leq i})$, by joining the successive vertices $P(\Lambda_1, \ldots, \Lambda_{i-1}, \Lambda_{ij})$ $1 \leq j \leq r_i$. Again by the normalization condition 3.6 Γ_i^2 is upperconvex. We do this for every cell of J until we reach atoms. In the end, we get polygonal lines satisfying

1) Vertices of Γ^i are contained in the set of vertices of Γ^{i+1},

2) A polygonal segment of Γ^{i+1} connecting two successive vertices of Γ^i is upperconvex,

3) The first polygonal line Γ^0 is the line segment connecting the origin to the point $P(\Lambda) = (k, n)$. Furthermore the last line Γ^s is $\Gamma(\Lambda_1, \Lambda_2, \ldots, \Lambda_m)$ where Λ_i are the atoms of the hierarchy J.

On this construction let $D^i = D^i(\Lambda_1, \Lambda_2, \ldots, \Lambda_m)$ $i > 0$, be the polygon bounded by the lines Γ^i and Γ^0. We know by the properties 1 through 3 that Γ^i intersects Γ^0 only at the endpoints. The difference $D^i - D^{i-1}$ $i > 1$ is a union of convex polygons, one for each side of Γ^i. Using those polygons we get a decomposition of $D^s = D$ into convex pieces

$$D = \cup_\alpha D_\alpha. \tag{3.9}$$

The boundary of a piece D_α consists of a side of some Γ^{i-1} and a polygonal segment that connects the two ends of that side. So the decomposition in 3.9 is obtained by cutting D using some of inner disjoint diagonals of D *i.e.* cutting by some of its diagonals that entirely lie in D, connecting nonadjacent vertices and having no common points except possibly the ends.

For a closer look at the coefficient a of 3.7 we use this geometric interpretation. We have observed that the polygonal line corresponding to a normalized hierarchy intersects the line segment Γ^0 only at the ends. This motivates the following

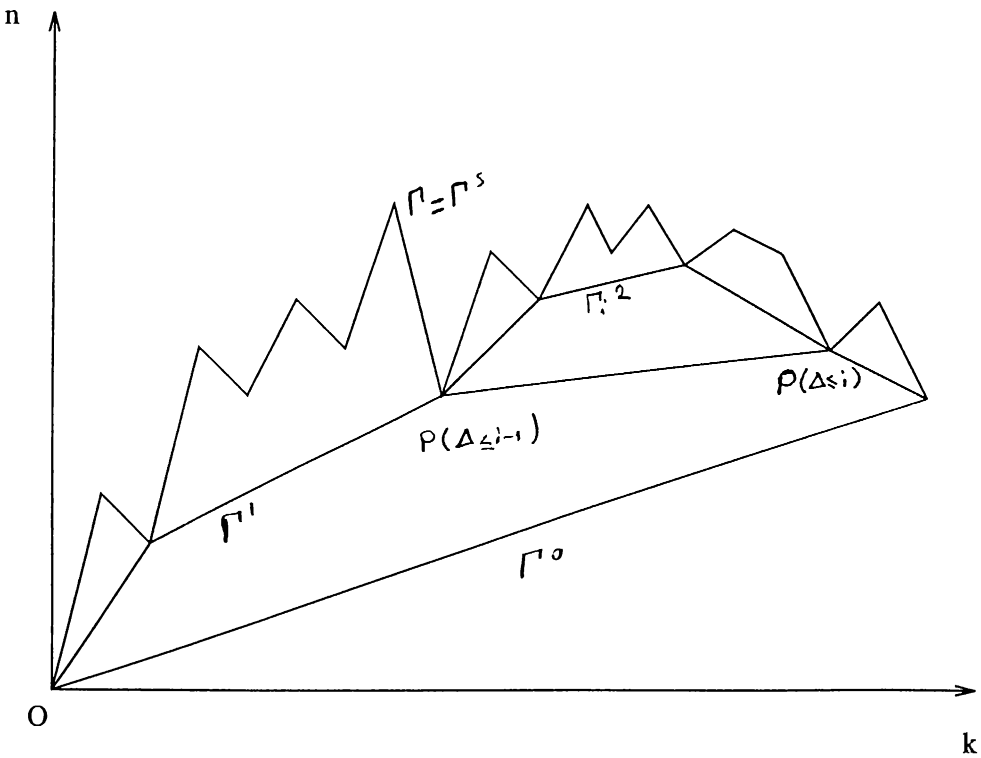


Figure 3.1: Normalized Hierarchy Represented on Plane

Definition 3.8 The decomposition $\Lambda = (\Lambda_1, \Lambda_2, \ldots, \Lambda_m)$ is said to be stable if the following relation for the slopes is satisfied

$$\mu(\Lambda_{\leq i}) > \mu(\Lambda) \quad 1 \leq i \leq m-1. \tag{3.10}$$

Proposition 3.9 *The coefficient $a(\Lambda_1, \Lambda_2, \ldots, \Lambda_m)$ is nonzero only for stable decompositions $\Lambda = (\Lambda_1, \Lambda_2, \ldots, \Lambda_m)$ into atoms Λ_i and in this situation*

$$a(\Lambda_1, \Lambda_2, \ldots, \Lambda_m) = h^+(D) - h^-(D),$$

where $h^+(h^-)$ is the number of partitions of the polygon D into even(resp. odd) number of convex pieces by the disjoint inner diagonals.

Proof: We have a sum in 3.8 over fixed sets of atoms of normalized hierarchies and a is defined as sum of signs of a number of normalized hierarchies with fixed set of atoms. Normalized hierarchies give stable decompositions as explained so a can not be nonzero for a nonstable decomposition. We have one-one correspondance between the normalized hierarchies and the subdivisions of D by its disjoint inside diagonals. The cells of positive level which are not atoms correspond to the diagonals of the decomposition. Each diagonal means one convex piece in such a decomposition.

$sign(J) = (-1)^{NA(J)} = (-1)^{\text{num. of convex pieces in decomposition } D_J}$

hence,

$$a(\Lambda_1, \Lambda_2, \ldots, \Lambda_m) = h^+(D) - h^-(D). \square$$

We still want to find the coefficient a in explicit form. We get help of the combinatorial geometry of the plane to find the relation between $h^+(D)$ and $h^-(D)$.

Let D be a plane polygon no three of its vertices lying on the same line. A diagonal of D is a line segment connecting nonadjacent vertices of D and lying entirely in D.

Proposition 3.10 *For $n > 3$ any n-gon D contains a diagonal.*

Proof: D contains a vertex B at which the angle is less than π. Take the adjacent angles A, B, C with this order. Now, if we can't draw a diagonal from B to a vertex $D \neq A, C$, then AC is a diagonal. If not, D is a triangle. $\square$

Corollary 3.11 *Any n-gon D can be divided by its disjoint inside diagonals into triangles. The number of such triangles in any such subdivision is $n-2$.*$\square$

Now, we want to learn more about the subdivisions s of D into any convex pieces. We denote by $\mathcal{S}$ the set of such subdivisions. This is an ordered set and $s < t$ means s is inscribed in t. So, the minimal elements of $\mathcal{S}$ are triangulations.

The key to find a in explicit form is the theorem following the next two propositions. We will imitate the steps in [Kly1] to prove this theorem. For this we develope the notations. Let D be a polygon and a be a side of D fixed. We denote by $\Delta = \Delta(a)$ the set of all convex polygons that are inscribed in D and contain the side a. By $|\delta|$ we denote the number of sides of a polygon δ.

Proposition 3.12 *For any convex polygon D, we have*

$$\sum_{\delta\in\Delta}(-1)^{|\delta|} = -1.$$

Proof: We fix the side a, hence for a k-gon $\delta \in \Delta(a)$, remain $k-2$ vertices which can be choosen among $n-2$ vertices of D. So we have $\binom{n-2}{k-2}$ k-gons in $\Delta(a)$. If we take sum over k

$$\sum_{\delta\in\Delta}(-1)^{|\delta|} = \sum_{k=3}^{n}\binom{n-2}{k-2}(-1)^{k-2}$$

$$= \sum_{k=1}^{n-2}\binom{n-2}{k}(-1)^{k} = (1-1)^{n-2} - 1 = -1.\square$$

Proposition 3.13 *For any polygon D, we have*

$$\sum_{\delta\in\Delta}(-1)^{|\delta|} = -1. \tag{3.11}$$

Proof: By induction reasons, we take 3.11 valid for m-gons where $m < |D|$. Let $V = V(a)$ be the set of vertices of D from which we can see the side $a = AB$. Take all theese vertices $C_1, C_2, \ldots, C_m$ in the order of increasing of the angle ABC_i and consider the polygon

$$D(a) = AC_1 \ldots C_m B.$$

By construction it follows that if $\delta \in \Delta(a)$ then it is contained in $D(a)$. Hence, if $D(a) \neq D$ then equation 3.11 follows from the induction hypothesis. If we have $D(a) = D$ for all a then D is convex and 3.11 is valid by the previous proposition. □

Theorem 3.14 *For any n-gon D*

$$h^+(D) - h^-(D) = (-1)^n.$$

Proof: Any subdivision $\sigma \in \Sigma(D)$ contains unique polygon $\delta \in \Delta$. Hence

$$\begin{aligned}
\chi(D) &= h^+(D) - h^-(D) \\
&= \sum_{\sigma \in \Sigma(D)} (-1)^{|\sigma|} \\
&= \sum_{\delta \in \Delta} \sum_{\delta \in \sigma \in \Sigma(D)} (-1)^{|\sigma|} \\
&= -\sum_{\delta \in \Delta} \prod_{D_i \in D \backslash \delta} \chi(D_i).
\end{aligned}$$

The product is taken over all components D_i in the complementation $D \backslash \delta$.By induction reasons we assume that the theorem is valid for the polygons D_i hence we have

$$\prod_{D_i \in D \backslash \delta} \chi(D_i) = \prod_{D_i \in D \backslash \delta} (-1)^{|D_i|} = (-1)^{|D|+|\delta|-2}.$$

Therefore

$$\begin{aligned}
\chi(D) = -\sum_{\delta \in \Delta} \prod_{D_i \in D \backslash \delta} \chi(D_i) &= -\sum_{\delta \in \Delta} (-1)^{|D|+|\delta|} \\
&= (-1)^{|D|} (-\sum_{\delta \in \Delta} (-1)^{|\delta|}) \\
&= (-1)^{|D|}. \square
\end{aligned}$$

If we put the coefficient a in its place we get

$$R_q(n,k) = \sum_{(n_0,k_0)(n_1,k_1)\ldots(n_m,k_m)} (-1)^m \begin{bmatrix} k \\ k_0 k_1 \ldots k_m \end{bmatrix}_q \binom{n}{n_0 n_1 \ldots n_m} q^{\sum_{i<j} k_i n_j} \prod_i [k_i]_q^{n_i}$$

where the sum runs over all *stable* decompositions of (n, k).

Theorem 3.15 *For coprime n and k, Poincaré polynomial of the moduli space $C_{n,k}$ is given by*

$$P_{n,k}(q) = \frac{1}{q^{\frac{k(k-1)}{2}}(q-1)^{n-1}[k]_q!} \sum_{(n_0,k_0)(n_1,k_1)\ldots(n_m,k_m)} (-1)^m \begin{bmatrix} k \\ k_0 k_1 \ldots k_m \end{bmatrix}_q \binom{n}{n_0 n_1 \ldots n_m} q^{\sum_{i<j} k_i n_j} \prod_i [k_i]_q! \quad (3.12)$$

where the sum is taken over all stable decomposition of (n,k).

Proof: The sum on the right hand side is the number of all stable n line configurations in a k dimensional vector space. A stable configuration has no pointwise automorphism other than the scalar ones, so we divide the sum by the cardinality of PGL_k to get the number of rational points of the moduli space.□

3.4 Sum over Geometric Terms

The decomposition in index of sum in 3.12 can be put in geometric terms. We denote by $k \times n$ a rectangle with horizontal dimension k and vertical dimension n units. *Diagonal* of the rectangle is the line segment that connects the South-west and the North-east corners. Also we will use the paths $\Gamma \subset k \times n$ running from South-west to North-east which lie over the diagonal. Our paths won't be allowed to move in the directions other than north and east. The points where the path changes its direction from east to north will be called a *vertex*. We can denote such paths with a decomposition as in

$$\begin{aligned} n_0 + n_1 + \ldots + n_m &= n, \\ k_0 + k_1 + \ldots + k_m &= k, \end{aligned}$$

where $k_i > 0$ is a horizontal step and $n_i \geq 0$ is a vertical step of the path Γ. Having introduced these notations, we can identify the decomposition of (n,k) in the index of the sum in 3.12 with our paths. And the area $S(\Gamma)$ over the path Γ is

$$S(\Gamma) = \sum_{i<j} k_i n_j$$

So we can rewrite Poincaré polynomial 3.12 as

$$P_{n,k}(q) = \frac{1}{q^{\frac{k(k-1)}{2}}(q-1)^{n-1}[k]_q!}\sum_{\Gamma}(-1)^m \left[\begin{array}{c} k \\ k_0k_1\dots k_m \end{array}\right]_q \left(\begin{array}{c} n \\ n_0n_1\dots n_m \end{array}\right) q^{S(\Gamma)}\prod_i [k_i]_q \quad (3.13)$$

where the sum runs over paths as described above.

3.4.1 Reduced Steps for Paths

We will try to achieve a simplification in 3.13 by excluding the successive horizontal steps of Γ i.e the zero vertical steps n_i. Calculations below are obtained from Kly2.

We call our first special polynomial in q *quantum Stirling numbers.* For $q = 1$ they give the classical Stirling numbers of the second kind $S(n, k)$(equal to the number of partitions of a set of $(n + k)$ elements into k nonempty clusters [Gon]). We define quantum Stirling numbers by the following explicit formula

$$S_q(n,k) := \frac{1}{q^{\frac{k(k-1)}{2}}[k]_q!}\sum_{i=0}^{k}(-1)^i q^{\frac{i(i-1)}{2}}[k-i]_q^{n+k}\left[\begin{array}{c} k \\ i \end{array}\right]_q.$$

$S_q(n, k)$ has the following properties which follow from the recurrence relation given below.

Proposition 3.16
1) $S_q(n,k)$ is a unitary polynomial in q with integer coefficients of degree $n(k-1)$ and free term $\binom{n+k-1}{n}$.
2) $S_q(0,k) = S_q(n,1) = 1$ and $S_q(n,k) \neq 0$ only for $k > 0, n \geq 0$ with only one exception $S_q(0,0) = 1$.
3) Recurrence relation:

$$S_q(n,k) = S_q(n,k-1) + [k]_q S_q(n-1,k).\square$$

We'll show that we can write the polynomial $P_{n,k}(q)$ by using $S_q(n, k)$ in the following form

Theorem 3.17

$$P_{n,k}(q) = \frac{n!}{(q-1)^{k-1}} \sum_{\Gamma} (-1)^m q^{S(\Gamma)} \frac{S_q(n_0,k_0)S_q(n_1,k_1)\dots S_q(n_m,k_m)}{(n_0+k_0)!(n_1+k_1)!\dots(n_m+k_m)!} \tag{3.14}$$

where the summation runs over all paths

$$\Gamma : n_0, k_0, n_1, k_1, \dots, n_m, k_m$$

above the diagonal of $k \times (n-k)$ rectangle with successive vertical and horizontal steps $n_i \geq 0$ and $k_i > 0$.

Proof: After a simple cacellation the formula 3.13 becomes

$$P_{n,k}(q) = \frac{1}{q^{\frac{k(k-1)}{2}}(q-1)^{k-1}} \sum_{\Gamma} (-1)^m q^{S(\Gamma)} \binom{n}{n_0 n_1 \dots n_m} \frac{\prod_i [k_i]_q^{n_i}}{\prod_i [k_i]_q!}$$

without any change in index of the sum. Now let us consider a vertical step $a > 0$ of Γ followed by a number of horizontal steps b_i of total length $b = \sum b_i$ having zero vertical steps between them. Most parts of the formula depends only on a and b. Instead of only $\frac{[b]_q^a}{[b]_q!}$ we have

$$\sum_{b_0+b_1+\dots+b_s=b} (-1)^s \frac{[b_0]_q^a}{[b_0]_q![b_1]_q!\dots[b_s]_q!} =_{b_0=b-p}$$

$$\frac{1}{[b]_q!} \sum_p [b-p]_q^a \begin{bmatrix} b \\ p \end{bmatrix}_q \sum_{b_1+b_2+\dots+b_s=p} (-1)^s \begin{bmatrix} p \\ b_1, b_2, \dots, b_s \end{bmatrix}_q$$

The following claim simplifies our job

Claim 3.18

$$\sum_{b_1+b_2+\dots+b_s=p} (-1)^s \begin{bmatrix} p \\ b_1, b_2, \dots, b_s \end{bmatrix}_q = (-1)^p q^{\frac{p(p-1)}{2}}.$$

Proof of claim: Left hand side is the coefficient of u^p in the following series

$$\sum_s \left[1 - \sum_{k\geq 0} \frac{u^k}{[k]_q!}\right]^s = \left[\sum_{k\geq 0} \frac{u^k}{[k]_q!}\right]^{-1} = \sum_{p\geq 0} (-1)^p q^{\frac{p(p-1)}{2}} \frac{u^p}{[p]_q!}$$

The last equality follows from the quantum binomial formula.

$$\sum_{p\geq 0} (-1)^p q^{\frac{p(p-1)}{2}} \begin{bmatrix} n \\ p \end{bmatrix}_q = 0, \quad n > 0. \square$$

So we arrive to the quantum Stirling numbers

$$\sum_{b_0+b_1+\ldots+b_s=b}(-1)^s\frac{[b_0]_q^a}{[b_0]_q![b_1]_q!\ldots[b_s]_q!}=$$
$$\frac{1}{[b]_q!}\sum_{p\geq 0}(-1)^p[b-p]_q^a\left[\begin{array}{c} b \\ p \end{array}\right]_q = q^{\frac{b(b-1)}{2}}S_q(a-b,b)$$

which allows us rewrite 3.13 as follows

$$P_{n,k}(q)=\frac{n!}{q^{\binom{k}{2}}(q-1)^{k-1}}\sum_{\Gamma}(-1)^m q^{S(\Gamma)+\sum\binom{k_i}{2}}\frac{S_q(n_0-k_0,k_0)\ldots S_q(n_m-k_m,k_m)}{n_0!\ldots n_m!}$$

The sum runs over all paths

$$\Gamma : n_0, k_0, n_1, k_1, \ldots, n_m, k_m$$

above the diagonal of the $k\times n$ rectangle with positive steps both in vertical and horizontal directions. Since $S_q(n-k,k)=0$ for $n<k$, we may suppose that $n_i\geq k_i$. This makes it natural to consider instead of Γ a new path $\tilde{\Gamma}$ in $k\times(n-k)$ rectangle with the same horizontal steps and reduced vertical steps n_i-k_i. Using

$$S(\Gamma)-S(\tilde{\Gamma})=\binom{k}{2}-\sum_i\binom{k_i}{2}$$

we arrive to the formula 3.14. □

We tried to get a formula without zero vertical steps of the paths but in the end the reduced steps n_i still can be zero. So we attack once more to the same problem with new polynomials. We introduce another quantum numbers (i.e. polynomials in q)

$$F_q(n,k)=\sum_{i\leq k}(-1)^{k-i}\binom{n+k}{n+i}S_q(n,i)$$

with the following properties.

Proposition 3.19
1. $F_q(n,k)$ is a unitary polynomial of degree $n(k-1)$ with integer coefficients and free term $(-1)^{k-1}$.
2. $F_q(n,k)=0$ except $n\geq 0, k>0$ and

$$F_q(0,k)=(-1)^{k-1},\ F_q(n,1)=1.$$

3. The following symmetry relation holds

$$\frac{F_q(n,k)}{(q-1)^k} = \frac{F_q(k,n)}{(q-1)^n}.$$

4. The following duality identity holds

$$\sum_\Gamma (-1)^m q^{S(\Gamma)} \frac{F_q(n_0,k_0)\dots F_q(n_m,k_m)}{(n_0+k_0)!\dots(n_m+k_m)!} = (-1)^{k-1}\frac{F_q^*(n,k)}{(n+k)!}$$

where the sum runs over all paths

$$\Gamma : n_0, k_0, \dots, n_m, k_m$$

from SW to NE corners of $k \times n$ rectangle with vertical and horizontal steps $n_i, k_j > 0$. Here $S(\Gamma)$ is the area above Γ and

$$F_q^*(n,k) = q^{n(k-1)} F_{\bar q}(n,k), \;\; \bar q = 1/q$$

is the dual polynomial to F_q. □

Theorem 3.20 *In the previous notations*

$$P_{n,k}(q) = \frac{n!}{(q-1)^{k-1}} \sum_\Gamma (-1)^m q^{S(\Gamma)} \frac{F_q(n_0,k_0)\dots F_q(n_m,k_m)}{(n_0+k_0)!\dots(n_m+k_m)!} \tag{3.15}$$

where the sum runs over all paths

$$\Gamma : n_0, k_0, , n_1, k_1, \dots, n_m, k_m$$

above the diagonal of $k \times (n-k)$ rectangle with successive vertical and horizontal steps $n_i > 0, \;\; k_i > 0$.

Proof: The proof is similar to calculations in the previous theorem.Let us consider a segment of the line Γ consisting of a vertical step of length n followed by a sequence of horizontal steps k_i of total length $k = \sum_i k_i$. Then summation over all partitions k_i of k changes in the formula 3.14 each multiplier $\frac{S_q(n,k)}{(n+k)!}$ to the sum

$$\sum_{k_0+k_1+\dots+k_s=k} (-1)^s \binom{n+k}{n+k_0, k_1, \dots, k_s} S_q(n,k) \;\; =$$

$$= \sum_{k_0 \le k} \binom{n+k}{n+k_0} S_q(n,k_0) \sum_{k_1+k_2+\dots+k_s=k-k_0} (-1)^s \binom{k-k_0}{n+k_1, k_2, \dots, k_s}$$

We can evaluate the internal sum

$$\begin{aligned}\sum_{k_1+k_2+\ldots+k_s=k-k_0}(-1)^s\binom{k-k_0}{n+k_1,k_2,\ldots,k_s} &=\\ k!(\text{coefficient of } z^k \text{ in } 1+(1-e^z)+(1-e^z)^2+\ldots) &=\\ k!(\text{coefficient of } z^k \text{ in } e^{-z}) &= (-1)^k\end{aligned}$$

So we get F polynomials

$$\begin{aligned}\sum_{k_0+k_1+\ldots+k_s=k}(-1)^s\binom{n+k}{n+k_0,k_1,\ldots,k_s}S_q(n,k_0) &=\\ \sum_{i\leq k}(-1)^{k-i}\binom{n+k}{n+i}S_q(n,i) &= F_q(n,k)\end{aligned}$$

and we can rewrite the formula 3.14 as stated in theorem. □

3.5 Mass Formula

In this section we give one of the applications of Poincaré polynomial in [Kly2]. Mass formula counts the equivalence classes of codes with an assigned weight reciprocal cardinality of automorphism group of the class.

In the previous sections we dealt with the space $C_{n,k}$ of ordered configurations. Both from geometric and code theoretical points of view it is more natural to deal with *unordered* configurations (codes differing by a permutation of coordinates are usually identified). They may be treated as points of the factor $C_{n,k}/S_n$ with respect to natural action of the symmetric group S_n by permutation of points. This factor is usually a singular variety. Besides a rational point of this factor doesn't necessarily correspond to a configuration of rational points.

In the following theorem we deal with unordered configurations of rational points upto projective equivalence rather than with rational points of the factor $C_{n,k}/S_n$.

Theorem 3.21 *For coprime n and k the following mass formula for unordered stable n point configurations $\Sigma \subset \mathbb{P}^{k-1}(\mathbb{F}_q)$ holds*

$$\sum_{\Sigma}\frac{1}{|Aut\Sigma|}=\frac{P_{n,k}(q)}{n!}$$

Proof: Let $\Sigma \in \mathcal{C}_{n,k}$ be a stable configuration of n points in $\mathbb{P}^{k-1}$. It corresponds to an equivalence class of codes. If we disregard its order and consider the unordered configuration $\Sigma \subset \mathbb{P}^{k-1}$ we get $n!$ different orderings but $\frac{n!}{|Aut\Sigma|}$ different classes of stable codes. Sum over all such unordered configurations of stable n point configurations gives us the number of stable $[n,k]_q$ codes upto equivalence which is given by $P_{n,k}(q)$. Hence we have

$$\sum_{\Sigma} \frac{n!}{|Aut\Sigma|} = P_{n,k}(q)$$

$$\sum_{\Sigma} \frac{1}{|Aut\Sigma|} = \frac{P_{n,k}(q)}{n!} \square$$

Chapter 4

Asymptotic Distribution of Stable Codes

We devote this chapter to an application of Poincaré polynomial $P_{n,k}(q)$ of theorem 3.15.This will be the achievement of proof of the main theorem in this chapter:

Theorem 4.1
$$\lim_{n,k\to\infty} \frac{\#(stable[n,k]_q codes)}{\#(all[n,k]_q codes)} = 1 \tag{4.1}$$
under the constraint
$$\epsilon < \frac{k}{n} < 1-\epsilon \qquad\qquad 0<\epsilon<1. \tag{4.2}$$

In words, we want to show that asymptotically all codes whose parameters n and k satisfy 4.2 ,which in turn is to say that almost all codes, are stable.

4.1 Poincaré Polynomial

In chapter 3, for coprime n and k we have obtained the Poincaré polynomial of the isomorphic varieties

$$G(n,k)//T^n \simeq (\mathbb{P}^{k-1})^n//PGL_k$$

[proposition 2.4]. This polynomial gives us the number of stable k spaces of $\mathbb{F}_q^n$ upto equivalence under the action of the multiplicative torus T^n . The following proposition shows how Poincaré polynomial $P_{n,k}(q)$ is involved for our purposes in this chapter.

Proposition 4.2 *The limit in theorem 4.1 is equivalent to*

$$\lim_{n,k\to\infty} \frac{P_{n,k}(q)(q-1)^{n-1}}{\begin{bmatrix} n \\ k \end{bmatrix}_q} \tag{4.3}$$

while the condition 4.2 is respected.

Proof: We need to find the number of stable $[n,k]_q$ codes. They are counted upto equivalence under the action of T^n by $P_{n,k}(q)$. In each orbit we have $(q-1)^{n-1}$ codes, because $q-1$ elements of T^n act trivially on subspaces. Hence we have

$$\#(\textit{all stable } [n,k]_q \textit{ codes}) = P_{n,k}(q)(q-1)^{n-1}.$$

The Gaussian multinomial coefficient counts the number of rational points of $G(n,k)$ over the field $\mathbb{F}_q$.

$$\#(\textit{all } [n,k]_q \textit{ codes}) = \begin{bmatrix} n \\ k \end{bmatrix}_q$$

So we have the equality

$$\frac{\#(\textit{allstable } [n,k]_q \textit{ codes})}{\#(\textit{all}[n,k]_q \textit{ codes})} = \frac{P_{n,k}(q)(q-1)^{n-1}}{\begin{bmatrix} n \\ k \end{bmatrix}_q}$$

which shows the result.□

4.2 Poincaré Duality

The limit in proposition 4.2 involves powers of q, the cardinality of the ground field. Poincaré duality will help us continue the calculations in $\bar{q} = \frac{1}{q}$.

Proposition 4.3 *The limit in theorem 4.1 is equivalent to*

$$\lim_{n,k\to\infty} \frac{P_{n,k}(\bar{q})(1-\bar{q})^{n-1}}{\begin{bmatrix} n \\ k \end{bmatrix}_{\bar{q}}} \tag{4.4}$$

with keeping the condition 4.2 on n and k.

Proof: Both $P_{n,k}(q)$ and the Gaussian multinomial coefficient in equation 4.3 are Poincaré polynomials hence we can use their selfdualities

$$\begin{aligned} P_{n,k}(q) &= q^{\dim(\mathcal{C}_{n,k})} P_{n,k}(\bar{q}) \\ \begin{bmatrix} n \\ k \end{bmatrix}_q, &= q^{\dim(G(n,k))} \begin{bmatrix} n \\ k \end{bmatrix}_{\bar{q}} \qquad \bar{q} = \frac{1}{q}. \end{aligned}$$

If we substitute this to equation 4.3, we get

$$\frac{q^{(k-1)(n-k-1)} P_{n,k}(\bar{q}) q^{n-1}(1-\bar{q})^{n-1}}{q^{k(n-k)} \begin{bmatrix} n \\ k \end{bmatrix}_{\bar{q}}} = \frac{P_{n,k}(\bar{q})(1-\bar{q})^{n-1}}{\begin{bmatrix} n \\ k \end{bmatrix}_{\bar{q}}}$$

whose limit under the condition 4.2 is equal to that in 4.1 by proposition 4.2. □

4.3 Asymptotics of Quantum Coefficients

Definition 4.4 The function

$$\eta(q) = \prod_{i=1}^{\infty} (1-q^i)$$

is absolutely convergent for $|q| < 1$ and is called the Etha function of Dedekind.

Using Poincaré duality and the Etha function, we can prove the following

Proposition 4.5 *Theorem 4.1 is equivalent to*

$$\lim_{n,k\to\infty} (1-\bar{q})^{n-1} P_{n,k}(\bar{q}) = \frac{1}{\eta(\bar{q})} \tag{4.5}$$

provided n, k are subjected to the constraint in 4.2.

Proof: We investigate

$$\lim_{n,k\to\infty}\begin{bmatrix} n \\ k \end{bmatrix}_{\bar{q}}$$

where k/n is seperated both from 0 and 1 by 4.2.

$$\begin{bmatrix} n \\ k \end{bmatrix}_{\bar{q}} = \frac{\prod_{i=1}^{n}(1-\bar{q}^i)}{\prod_{j=1}^{k}(1-\bar{q}^j)\prod_{l=1}^{n-k}(1-\bar{q}^l)} \tag{4.6}$$

Since $n-k$ too tends to infinity as well as n and k do, we have

$$\lim_{n,k\to\infty}\begin{bmatrix} n \\ k \end{bmatrix}_{\bar{q}} = \frac{1}{\eta(\bar{q})}.$$

Hence we are done by proposition 4.3. □

4.4 Formal Limit

We will carry out the calculations in new quantum numbers defined by

$$\sigma_q(n,k) := (1-q)^n q^{n(k-1)} S_{\bar{q}}(n,k).$$

Proposition 4.6
1) $\sigma_q(n,k)$ is a polynomial in q with integer coefficients.It has degree kn and free term 1.
2)$\sigma_q(n,k)$ satisfies the recurrence relation

$$\sigma_q(n,k) = q^k\sigma_q(n,k-1) + (1-q^k)\sigma_q(n-1,k).$$

Proof: Those follow at once from proposition 3.16 items 1 and 3. □

Using σ polynomials, we will put $P_{n,k}(q)$ in a more convenient form for our objectives.

Proposition 4.7 *We can write Poincaré polynomial of moduli space $\mathcal{C}_{\backslash,\|}$*

$$P_{n,k}(q) = \frac{n!}{(1-q)^{n-1}}\sum_{\Gamma}(-1)^m q^{S^*(\Gamma)}\frac{\sigma_q(n_0,k_0)\sigma_q(n_1,k_1)\ldots\sigma_q(n_m,k_m)}{(n_0+k_0)!(n_1+k_1)!\ldots(n_m+k_m)!} \tag{4.7}$$

where index of sum is the same as in equation 3.14 but

$$S^*(\Gamma) = k(n-k) - \sum_{i\le j} k_i n_j$$

for any path $\Gamma : n_0, k_0, n_1, k_1, \ldots, n_m, k_m.$

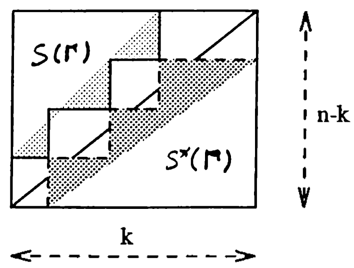


Figure 4.1: $S^*(\Gamma)$

Proof: We begin with formula given in 3.14 and use the definition of σ polynomials. After multiplying and dividing each $S_q(n,k)$ by $\bar{q}^{n(k-1)}(1-\bar{q})^n$ we get the result at once by Poincaré duality. □

We need the following important estimation on $S^*(\Gamma)$.

Lemma 4.8 *For any path* Γ *in index of sum of equation 4.7 we have*

$$S^*(\Gamma) \geq n - k + 1 - [\frac{n}{k}]$$

except for the trivial one

$$\Gamma_0 : n-k, k \qquad \textit{with} \qquad S^*(\Gamma) = 0.$$

Proof: A path Γ has vertices at integer pairs (x, y) over the diagonal of the $k \times (n-k)$ rectangle. We fix such a vertex and try to estimate the area $(k-x)y$ from below. To find the minimum of this value, we have to choose y as close to the diagonal as possible over a given x.

$$y = [(\frac{n-k}{k})x] + 1$$

This choice works because there is no vertex *on* the diagonal, except the two ends of the paths. So, the area enclosed is

$$([(\frac{n-k}{k})x] + 1)(k - x)$$

This quantity becomes smallest with the choice $x = k-1$ and we get the result. □

Lemma 4.9

$$\lim_{n,k\to\infty} \sigma_{\bar{q}}(n-k,k) = \frac{1}{\eta(\bar{q})} \tag{4.8}$$

provided conditions of equation 4.2 are respected.

Proof: The crucial point is observing that

$$\sigma_q(n,k) \;=\; \sum_{i=0}^{k}(-1)^i \frac{q^{\frac{i}{2}(2n+i+1)}(1-q^{k-i})^{n+k}}{(1-q)\dots(1-q^i)(1-q)\dots(1-q^{k-i})}.$$

Hence we have

$$\sigma_{\bar{q}}(n-k,k) = \frac{(1-\bar{q}^k)^n}{(1-\bar{q})(1-\bar{q}^2)\dots(1-\bar{q}^k)} + \sum_{i=1}^{k}(-1)^i \frac{\bar{q}^{\frac{i}{2}(2(n-k)+i+1)}(1-\bar{q}^{k-i})^n}{(1-\bar{q})\dots(1-\bar{q}^i)(1-\bar{q})\dots(1-\bar{q}^{k-}}$$

We estimate the sum on the right hand side.

$$\begin{aligned} \left|\sum_{i=1}^{k}(-1)^i \frac{\bar{q}^{\frac{i}{2}(2(n-k)+i+1)}(1-\bar{q}^{k-i})^n}{(1-\bar{q})\dots(1-\bar{q}^i)(1-\bar{q})\dots(1-\bar{q}^{k-i})}\right| &\le \frac{1}{\eta(\bar{q})}\sum_{i=1}^{k}\bar{q}^{i(n-k)} \\ &= \frac{\bar{q}^{n-k}}{\eta(\bar{q})}\sum_{i=1}^{k}\bar{q}^{(i-1)(n-k)}. \end{aligned}$$

The sum is convergent and the expression gets exponentially small as we let n and k to ∞ under the constraint of equation 4.2. Hence under the given conditions, we have

$$\lim_{n,k\to\infty}\sigma_{\bar{q}}(n-k,k) = \lim_{n,k\to\infty}\frac{(1-\bar{q}^k)^n}{(1-\bar{q})(1-\bar{q}^2)\dots(1-\bar{q}^k)} = \frac{1}{\eta(\bar{q})}.\Box$$

Now we show that limit in proposition 4.5 exists as formal power series.

Proposition 4.10

$$\lim_{n,k\to\infty}(1-\bar{q})^{n-1}P_{n,k}(\bar{q})$$

keeping the conditions of equation 4.2 on n and k exists as formal power series and is equal to that of $\frac{1}{\eta(\bar{q})}$.

Proof: The previous two lemmas left little to show. By lemma 4.8 we have

$$(1-\bar{q})^{n-1}P_{n,k}(\bar{q}) \equiv \sigma_{\bar{q}}(n-k,k) \bmod \deg N = n-k+[\frac{n}{k}]-1.$$

If we take limit we get

$$\lim_{n,k\to\infty}(1-\bar{q})^{n-1}P_{n,k}(\bar{q}) = \frac{1}{\eta(\bar{q})}$$

as formal power series by the lemma 4.9. $\Box$

We have to make finer estimations on $S^*(\Gamma)$ to show that the value of this limit as real number exists and is equal to $\frac{1}{\eta(\bar{q})}$.

4.5 Genuine Limit

It is in this section that we prove theorem 4.1 in full. Once more we enjoy new quantum numbers φ and new form of the Poincaré polynomial $P_{n,k}(q)$. We introduce new polynomial in q by

$$\varphi_q(n,k) = (1-q)^n q^{n(k-1)} F_{\bar{q}}(n,k).$$

Proposition 4.11

1) $\varphi_q(n,k)$ is a polynomial in q of degree nk, with integer coefficients and leading coefficient $(-1)^{n+k-1}$. It has constant term 1.

2)

$$\varphi_q(n,k) = \sum_{i=0}^{k}(-1)^{k-i} q^{n(k-i)} \binom{n+k}{n+i} \sigma_q(n,i). \tag{4.9}$$

3) $\varphi_q(n,k) = 0$ except for $n \geq 0$, $k > 0$ and

$$\varphi_q(0,k) = (-1)^{k-1}, \varphi_q(n,1) = (1-q)^n$$

4) $\varphi_q(n,k)$ satisfies the symmetry relation

$$\varphi_q(n,k) = \varphi_q(k,n). \square$$

Proposition 4.12 *We can express Poincaré polynomial $P_{n,k}(q)$ in terms of φ polynomials as*

$$P_{n,k}(q) = \frac{n!}{(1-q)^{n-1}} \sum_{\Gamma} (-1)^m q^{S^*(\Gamma)} \frac{\varphi_q(n_0,k_0)\varphi_q(n_1,k_1)\ldots\varphi_q(n_m,k_m)}{(n_0+k_0)!(n_1+k_1)!\ldots(n_m+k_m)!} \tag{4.10}$$

where index of sum is the same as in theorem 3.20.

Proof: Similar to proof of proposition 4.7, we take Poincaré polynomial given in equation 3.15 and multiply each $F_q(n,k)$ by $(1-\bar{q})^n \bar{q}^{n(k-1)}$. We get the result by Poincaré duality. $\square$

Proposition 4.13 *When n and k are under conditions of equation 4.2*

$$\lim_{n,k\to\infty} \varphi_{\bar{q}}(n,k) = \frac{1}{\eta(\bar{q})}.$$

Proof: We use boundedness of $\sigma(n,k)$ (lemma 4.9) and the identity given in equation 4.9 to show that φ and σ behave the same for big n and k.

$$\begin{aligned}\varphi_{\bar{q}}(n,k) &= \sum_{i=0}^{k}(-1)^{k-i}\bar{q}^{n(k-i)}\binom{n+k}{n+i}\sigma_{\bar{q}}(n,i)\\ &= \sigma_{\bar{q}}(n,k)+\sum_{j=1}^{k}(-1)^{j}\bar{q}^{nj}\binom{n+k}{j}\sigma_{\bar{q}}(n,k-j)\end{aligned}$$

Now we show that under the given conditions, the sum on the right hand side approaches to 0.

$$\begin{aligned}&|\sum_{j=1}^{k}(-1)^{j}\bar{q}^{nj}\binom{n+k}{j}\sigma_{\bar{q}}(n,k-j)|\\ &\leq A\sum_{j=1}^{n+k}\binom{n+k}{j}\bar{q}^{nj} = A((1+\bar{q}^{n})^{n+k}-1)\\ &= A(\bar{q}^{n})((1+\bar{q}^{n})+(1+\bar{q}^{n})^{2}+\ldots+(1+\bar{q}^{n})^{n+k-1})\\ &\leq A(\bar{q}^{n})(n+k-1)(1+\bar{q}^{n})^{n+k-1}\\ &= \exp\{n(-\log q+\frac{\log A(n+k-1)}{n}+(1+R-\frac{1}{n})\log(1+\bar{q}^{n})\}.\end{aligned}$$

We see that as n tends to infinity the identity approaches to 0. Hence under the conditions of equation 4.2 we have

$$\lim_{n,k\to\infty}\varphi_{\bar{q}}(n,k)=\lim_{n,k\to\infty}\sigma_{\bar{q}}(n,k)=\frac{1}{\eta(\bar{q})}$$

by lemma 4.9. □

We have seen that theorem 4.1 is equivalent to showing

$$\lim_{n,k\to\infty}(1-\bar{q})^{n-1}P_{n,k}(\bar{q})=\frac{1}{\eta(\bar{q})}$$

where n and k are under the conditions of equation 4.2 (Proposition 4.5). This is partly shown by proposition 4.10. We prove theorem 4.1 by showing that limit above exists as a real number and is equal to $\frac{1}{\eta(\bar{q})}$.

Proposition 4.14

$$\lim_{n,k\to\infty}(1-\bar{q})^{n-1}P_{n,k}(\bar{q})=\frac{1}{\eta(\bar{q})}$$

where condition in equation 4.2 is respected.

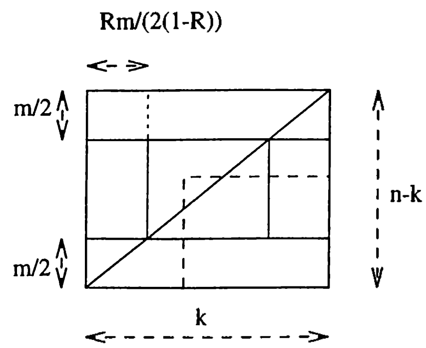


Figure 4.2:

Proof: Our estimations will be highly depending on the number $(m+1)$ of steps of the paths Γ_m. We recall that there is only one path

$$\Gamma_0 = n-k, k$$

with one step. We seperate the particular term corresponding to Γ_0 from the rest.

$$\begin{aligned}
&(1-\bar{q})^{n-1}P_{n,k}(\bar{q}) = \\
&= \sum_{\Gamma}(-1)^m \bar{q}^{S^*(\Gamma)} \binom{n}{n_0+k_0 \ldots n_m+k_m} \varphi_{\bar{q}}(n_0,k_0)\ldots\varphi_{\bar{q}}(n_m,k_m) \\
&= \varphi_{\bar{q}}(n-k,k) + \sum_m \sum_{\Gamma_m} (-1)^m \bar{q}^{S^*(\Gamma_m)} \binom{n}{n_0+k_0 \ldots n_m+k_m} \varphi_{\bar{q}}(n_0,k_0)\ldots\varphi_{\bar{q}}(n_m,k_m
\end{aligned}$$

We will estimate the sum on the right hand side. First we do this for big values of m. Consider division of the $k \times n-k$ rectangle as in figure 4.2.

Since the paths of the formula have positive steps, then for a fixed m a path Γ_m must have a vertex in the inner strip. Such a vertex help us for the following estimation

$$S^*(\Gamma) \geq \frac{m}{2}(k - \frac{mR}{2(1-R)}).$$

The number of all paths above the diagonal of the $(k \times n-k)$ rectangle (for n, k coprime) running from Southwest corner to Northeast is given by

$$\frac{1}{n}\binom{n}{k}. \tag{4.11}$$

which is less than 2^n. Hence we can estimate the sum above in the following way

$$
\begin{aligned}
&|\sum_m \sum_{\Gamma_m} (-1)^m q^{S^*(\Gamma_m)} \binom{n}{n_0+k_0 \dots n_m+k_m} \varphi_{\bar{q}}(n_0,k_0)\dots\varphi_{\bar{q}}(n_m,k_m)| \\
&\leq \sum_m A^{m+1} 2^n (m+1)^n \bar{q}^{\frac{m}{2}(k-\frac{mR}{2(1-R)})} \\
&= \sum_m \exp\left((m+1)\log A + n\log 2 + n\log(m+1) - \frac{m}{2}(k - \frac{mR}{2(1-R)})\log q\right) \\
&= \sum_m \exp\left(n(\log(m+1) - \frac{mR\log q}{2} + \frac{m^2 R\log q}{4n(1-R)} + \log 2 + \frac{(m+1)\log A}{n}\right).
\end{aligned}
$$

The information we need is in the first two terms of the exponent above. As n tends to infinity the rest becomes small comparing to them. There exists a constant

$$m_0 = m_0(q, R)$$

such that for $m \geq m_0$,

$$|\sum_m \sum_{\Gamma_m} (-1)^m q^{S^*(\Gamma_m)} \binom{n}{n_0+k_0 \dots n_m+k_m} \varphi_{\bar{q}}(n_0,k_0)\dots\varphi_{\bar{q}}(n_m,k_m)| = o(n).$$

We turn our attention to those paths Γ_m with $m < m_0$. We choose a number M satisfying

$$M > \frac{\log(m_0+1)}{R\log q}.$$

Now we consider the two cases

1) Γ_m has a vertex in the central strip described in the figure 4.3,
2) Γ_m has no vertex in the same strip.

Beginning with the first case, we have estimation for $S^*(\Gamma_m)$ as in

$$S^*(\Gamma_m) \geq M(k - \frac{RM}{1-R}).$$

Together with the reasonings above we have

$$
\begin{aligned}
&|\sum_{m<m_0} \sum_{\Gamma_m} (-1)^m q^{S^*(\Gamma_m)} \binom{n}{n_0+k_0 \dots n_m+k_m} \varphi_{\bar{q}}(n_0,k_0)\dots\varphi_{\bar{q}}(n_m,k_m)| \\
&\leq \sum_{m<m_0} 2^n A^{m_0+1} \bar{q}^{M(k-\frac{RM}{1-R})}(m_0+1)^n \\
&= \sum_{m<m_0} \exp\{n\log(2) + (m_0+1)\log(A) - M(k - \frac{RM}{1-R})\log(q) + n\log(m_0+1)\} \\
&= \sum_{m<m_0} \exp\{n(\log(m_0+1) - RM\log(q) + \frac{RM^2}{n(1-R)}\log(q) + \frac{m_0+1}{n}\log(A))\}.
\end{aligned}
$$

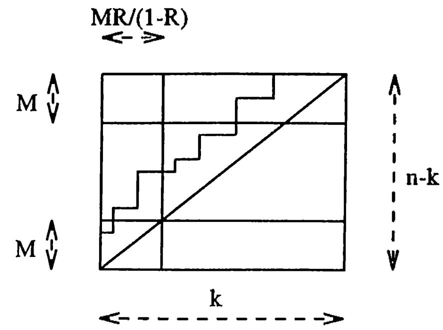


Figure 4.3:

Again we read from the first two terms of the exponent that by the choice 4.12 of M we have exponentially small sum for the paths of the first kind described above.

The latter case, where we deal with paths having no vertices in the central strip, helps us estimate Binomial coefficients. In this situation we have

$$n - (n_i + k_i) \leq 2M \qquad \text{for some i}$$

hence,

$$\binom{n}{n_0 + k_0 \ldots n_m + k_m} \leq \frac{n!}{(n_m + k_m)!} \leq n(n-1)\ldots(n-2M+1).$$

The last inequality means that the Binomial coefficient of the Poincaré polynomial is a polynomial in n of degree at most $2M$.

We have another estimation for the number of paths in this case. Since the steps of the paths are positive, the number of steps can not be more than $2M+1$. The number of paths in the upper strip is certainly less than

$$\sum_{j=1}^{M}(k-j)^j.$$

The number of paths which can be constructed in the triangular region of the lowest strip is bounded. Hence the number of paths in this case is less than the value of a polynomial $R_M(k)$ in k whose degree is no more than M.

It seems that, in this case our estimation for $S^*(\Gamma)$ given by

$$S^*(\Gamma) \geq n - k + [\frac{n}{k}] - 1$$

(lemma 4.8) is sufficient for our purposes.

Our final estimation is as follows

$$\sum_{\Gamma}(-1)^m q^{S^*(\Gamma)} \binom{n}{n_0+k_0 \ldots n_m+k_m} \varphi_{\bar{q}}(n_0,k_0)\ldots\varphi_{\bar{q}}(n_m,k_m)|$$
$$\leq A^{m_0+1} n(n-1)\ldots(n-2M+1)R_M(k)\bar{q}^{n-k+[\frac{n}{k}]-1}$$
$$\simeq \exp\{-(n-k+[\frac{n}{k}]-1)\log(q)+2M\log n+(m_0+1)\log A+M\log k\}$$
$$\leq \exp\{n(-(1-R+\frac{[\frac{1}{R}]}{k}-\frac{1}{n})\log(q)+\frac{2M\log n}{n}+\frac{M\log k}{n}+\frac{(m_0+1)\log A}{n})\}$$

As n tends to ∞ the terms in the exponent except the first tend to 0. The sum is exponentially small and tending to 0.

In the end keeping the condition 4.2 on n and k we came to the point

$$\begin{aligned}(1-\bar{q})^{n-1}P_{n,k}(\bar{q}) &= \varphi_{\bar{q}}(n-k,k)+o(n)\\ \lim_{n,k\to\infty}(1-\bar{q})^{n-1}P_{n,k}(\bar{q}) &= \frac{1}{\eta(\bar{q})}\end{aligned}$$

by the previous lemma.□

Theorem 4.1

$$\lim_{n,k\to\infty}\frac{\#(stable[n,k]_q codes)}{\#(all[n,k]_q codes)}=1$$

under the constraint

$$\epsilon<\frac{k}{n}<1-\epsilon \qquad\qquad 0<\epsilon<1.$$

Proof: We have shown by proposition 4.5 that theorem 4.1 is equivalent to

$$\lim_{n,k\to\infty}(1-\bar{q})^{n-1}P_{n,k}(\bar{q})=\frac{1}{\eta(\bar{q})}$$

provided n, k are subjected to the constraint in 4.2. This is proved by the previous proposition, hence we are done. □

Appendix A

Examples of Poincaré Polynomial and Mass

In this part, we give examples of Poincaré polynomials of the varieties $C_{n,k}$ for different choices of n and k. Also masses of stable $[n,k]_q$ codes for a variety of n, k and q are shown in a table.

We give also list of a Maple program which evaluates Poincaré polynomial of the variety $C_{n,k}$ for given n and k. Ibrahim Özen is highly indebted to professor Alexander A. Klyachko for providing this program. It is possible to evaluate $P_{n,k}(q)$ even for noncoprime n and k by this program. We have made use of it to give examples for this case too.

A.1 Examples of $P_{n,k}(q)$

$\mathbf{P}_{5,2}(q) = q^2 + 5\,q + 1$

$\mathbf{P_{7,2}(q)} = q^4 + 7\,q^3 + 22\,q^2 + 7\,q + 1$

$\mathbf{P_{7,3}(q)} = q^6 + 7\,q^5 + 29\,q^4 + 64\,q^3 + 29\,q^2 + 7\,q + 1$

$\mathbf{P_{8,3}(q)} = q^8 + 8\,q^7 + 37\,q^6 + 121\,q^5 + 227\,q^4 + 121\,q^3 + 37\,q^2 + 8\,q + 1$

$\mathbf{P_{9,2}(q)} = q^6 + 9\,q^5 + 37\,q^4 + 93\,q^3 + 37\,q^2 + 9\,q + 1$

$\mathbf{P_{9,4}(q)} = q^{12} + 9\,q^{11} + 46\,q^{10} + 175\,q^9 + 506\,q^8 + 1138\,q^7 + 1727\;,q^6 + 1138\,q^5 +$

$506\,q^4 + 175\,q^3 + 46\,q^2 + 9\,q + 1$

$\mathbf{P_{10,3}(q)} = q^{12} + 10\,q^{11} + 56\,q^{10} + 221\,q^9 + 681\,q^8 + 1608\,q^7 + 2527\,q^6 + 1608\,q^5 + 681\,q^4 + 221\,q^3 + 56\,q^2 + 10\,q + 1$

$\mathbf{P_{11,2}(q)} = q^8 + 11\,q^7 + 56\,q^6 + 176\,q^5 + 386\,q^4 + 176\,q^3 + 56\,q^2 + 11\,q + 1$

$\mathbf{P_{11,3}(q)} = q^{14} + 11\,q^{13} + 67\,q^{12} + 287\,q^{11} + 958\,q^{10} + 2630\,q^9 + 56 56\,q^8 + 8383\,q^7 + 5656\,q^6 + 2630\,q^5 + 958\,q^4 + 287\,q^3 + 6 7\,q^2 + 11\,q + 1$

$\mathbf{P_{11,4}(q)} = q^{18} + 11\,q^{17} + 67\,q^{16} + 298\,q^{15} + 1069\,q^{14} + 3257\,q^{13} + 8484\,q^{12} + 18801\,q^{11} + 34202\,q^{10} + 44937\,q^9 + 34202\,q^8 + 18801\,q^7 + 8484\,q^6 + 3257\,q^5 + 1069\,q^4 + 298\,q^3 + 67\,q^2 + 11\,q + 1$

$\mathbf{P_{11,5}(q)} = q^{20} + 11\,q^{19} + 67\,q^{18} + 298\,q^{17} + 1080\,q^{16} + 3313\,q^{15} + 8770\,q^{14} + 20253\,q^{13} + 40352\,q^{12} + 67279\,q^{11} + 84792\,q^{10} + 67279\,q^9 + 40352\,q^8 + 20253\,q^7 + 8770\,q^6 + 3313\,q^5 + 1080\,q^4 + 298\,q^3 + 67\,q^2 + 11\,q + 1$

$\mathbf{P_{12,5}(q)} = q^{24} + 12\,q^{23} + 79\,q^{22} + 377\,q^{21} + 1457\,q^{20} + 4824\,q^{19} + 14078\,q^{18} + 36794\,q^{17} + 86748\,q^{16} + 183912\,q^{15} + 342941\,q^{14} + 536640\,q^{13} + 644959\,q^{12} + 536640\,q^{11} + 342941\,q^{10} + 183912\,q^9 + 86748\,q^8 + 36794\,q^7 + 14078\,q^6 + 4824\,q^5 + 1457\,q^4 + 377\,q^3 + 79\,q^2 + 12\,q + 1$

$\mathbf{P_{13,2}(q)} = q^{10} + 13\,q^9 + 79\,q^8 + 299\,q^7 + 794\,q^6 + 1586\,q^5 + 794\,q^4 + 299\,q^3 + 79\,q^2 + 13\,q + 1$

$\mathbf{P_{13,3}(q)} = q^{18} + 13\,q^{17} + 92\,q^{16} + 456\,q^{15} + 1756\,q^{14} + 5552\,q^{13} + 14926\,q^{12} + 34243\,q^{11} + 63923\,q^{10} + 87518\,q^9 + 63923\,q^8 + 34243\,q^7 + 14926\,q^6 + 5552\,q^5 + 1756\,q^4 + 456\,q^3 + 92\,q^2 + 13\,q + 1$

$\mathbf{P_{13,4}(q)} = q^{24} + 13\,q^{23} + 92\,q^{22} + 469\,q^{21} + 1913\,q^{20} + 6592\,q^{19} + 19841\,q^{18} + 53055\,q^{17} + 126936\,q^{16} + 270975\,q^{15} + 509227\,q^{14} + 808616\,q^{13} + 988720\,q^{12} + 808616\,q^{11} + 509227\,q^{10} + 270 975\,q^9 + 126936\,q^8 + 53055\,q^7 + 19841\,q^6 + 6592\,q^5 + 1913\,q^4 + 469\,q^3 + 92\,q^2 + 13\,q + 1$

$\mathbf{P_{13,5}(q)} = q^{28} + 13\,q^{27} + 92\,q^{26} + 469\,q^{25} + 1926\,q^{24} + 6749\,q^{23} + 20881\,q^{22} + 58256\,q^{21} + 148257\,q^{20} + 346090\,q^{19} + 740967\,q^{18} + 1441861\,q^{17} + 2497242\,q^{16} + 3688314\,q^{15} + 4307297\,q^{14} + 3688314\,q^{13} + 2497242\,q^{12} + 1441861\,q^{11} + 740967\,q^{10} + 3460 90\,q^9 + 148257\,q^8 + 58256\,q^7 + 20881\,q^6 + 6749\,q^5 + 1926\,q^4 + 469\,q^3 + 92\,q^2 + 13\,q + 1$

A.2 Examples of Masses of stable $[n,k]_q$ codes

	q=2	q=3	q=4
$M_{3,1}(q)$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$
$M_{3,2}(q)$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$
$M_{4,1}(q)$	$\frac{1}{24}$	$\frac{1}{24}$	$\frac{1}{24}$
$M_{4,2}(q)$	$\frac{1}{8}$	$\frac{1}{6}$	$\frac{5}{24}$
$M_{4,3}(q)$	$\frac{1}{24}$	$\frac{1}{24}$	$\frac{1}{24}$
$M_{5,1}(q)$	$\frac{1}{120}$	$\frac{1}{120}$	$\frac{1}{120}$
$M_{5,2}(q)$	$\frac{1}{8}$	$\frac{5}{24}$	$\frac{37}{120}$
$M_{5,3}(q)$	$\frac{1}{8}$	$\frac{5}{24}$	$\frac{37}{120}$
$M_{5,4}(q)$	$\frac{1}{120}$	$\frac{1}{120}$	$\frac{1}{120}$
$M_{6,1}(q)$	$\frac{1}{720}$	$\frac{1}{720}$	$\frac{1}{720}$
$M_{6,2}(q)$	$\frac{1}{16}$	$\frac{5}{36}$	$\frac{37}{144}$
$M_{6,3}(q)$	$\frac{7}{48}$	$\frac{65}{144}$	$\frac{259}{240}$
$M_{6,4}(q)$	$\frac{1}{16}$	$\frac{5}{36}$	$\frac{37}{144}$
$M_{6,5}(q)$	$\frac{1}{720}$	$\frac{1}{720}$	$\frac{1}{720}$
$M_{7,1}(q)$	$\frac{1}{5040}$	$\frac{1}{5040}$	$\frac{1}{5040}$
$M_{7,2}(q)$	$\frac{5}{144}$	$\frac{7}{72}$	$\frac{31}{144}$
$M_{7,3}(q)$	$\frac{31}{112}$	$\frac{97}{72}$	$\frac{7759}{1680}$
$M_{7,4}(q)$	$\frac{31}{112}$	$\frac{97}{72}$	$\frac{7759}{1680}$
$M_{7,5}(q)$	$\frac{5}{144}$	$\frac{7}{72}$	$\frac{31}{144}$
$M_{7,6}(q)$	$\frac{1}{5040}$	$\frac{1}{5040}$	$\frac{1}{5040}$
$M_{8,1}(q)$	$\frac{1}{40320}$	$\frac{1}{40320}$	$\frac{1}{40320}$
$M_{8,2}(q)$	$\frac{5}{384}$	$\frac{7}{144}$	$\frac{155}{1152}$
$M_{8,3}(q)$	$\frac{39}{128}$	$\frac{2927}{1152}$	$\frac{5129}{384}$
$M_{8,4}(q)$	$\frac{465}{896}$	$\frac{485}{72}$	$\frac{131903}{2688}$
$M_{8,5}(q)$	$\frac{39}{128}$	$\frac{2927}{1152}$	$\frac{5129}{384}$
$M_{8,6}(q)$	$\frac{5}{384}$	$\frac{7}{144}$	$\frac{155}{1152}$
$M_{8,7}(q)$	$\frac{1}{40320}$	$\frac{1}{40320}$	$\frac{1}{40320}$
$M_{9,1}(q)$	$\frac{1}{362880}$	$\frac{1}{362880}$	$\frac{1}{362880}$
$M_{9,2}(q)$	$\frac{53}{10368}$	$\frac{251}{10368}$	$\frac{839}{10368}$
$M_{9,3}(q)$	$\frac{91}{384}$	$\frac{38051}{10368}$	$\frac{35903}{1152}$
$M_{9,4}(q)$	$\frac{13135}{8064}$	$\frac{447911}{10368}$	$\frac{208822469}{362880}$
$M_{9,5}(q)$	$\frac{13135}{8064}$	$\frac{447911}{10368}$	$\frac{208822469}{362880}$
$M_{9,6}(q)$	$\frac{91}{384}$	$\frac{38051}{10368}$	$\frac{35903}{1152}$
$M_{9,7}(q)$	$\frac{53}{10368}$	$\frac{251}{10368}$	$\frac{839}{10368}$
$M_{9,8}(q)$	$\frac{1}{362880}$	$\frac{1}{362880}$	$\frac{1}{362880}$

	q=2	q=3	q=4
$M_{10,1}(q)$	$\frac{1}{3628800}$	$\frac{1}{3628800}$	$\frac{1}{3628800}$
$M_{10,2}(q)$	$\frac{53}{34560}$	$\frac{251}{25920}$	$\frac{839}{20736}$
$M_{10,3}(q)$	$\frac{4579}{20736}$	$\frac{115651}{20736}$	$\frac{1477351}{20736}$
$M_{10,4}(q)$	$\frac{11933}{3840}$	$\frac{2522407}{12960}$	$\frac{107557223}{20736}$
$M_{10,5}(q)$	$\frac{81437}{16128}$	$\frac{54197231}{103680}$	$\frac{71208461929}{3628800}$
$M_{10,6}(q)$	$\frac{11933}{3840}$	$\frac{2522407}{12960}$	$\frac{107557223}{20736}$
$M_{10,7}(q)$	$\frac{4579}{20736}$	$\frac{115651}{20736}$	$\frac{1477351}{20736}$
$M_{10,8}(q)$	$\frac{53}{34560}$	$\frac{251}{25920}$	$\frac{839}{20736}$
$M_{10,9}(q)$	$\frac{1}{3628800}$	$\frac{1}{3628800}$	$\frac{1}{3628800}$
$M_{11,1}(q)$	$\frac{1}{39916800}$	$\frac{1}{39916800}$	$\frac{1}{39916800}$
$M_{11,2}(q)$	$\frac{3}{6400}$	$\frac{979}{259200}$	$\frac{9953}{518400}$
$M_{11,3}(q)$	$\frac{3263}{20736}$	$\frac{144101}{20736}$	$\frac{321073}{2304}$
$M_{11,4}(q)$	$\frac{1303}{256}$	$\frac{15734927}{20736}$	$\frac{853191289}{20736}$
$M_{11,5}(q)$	$\frac{2000669}{80640}$	$\frac{516049829}{71280}$	$\frac{26824927062749}{39916800}$
$M_{11,6}(q)$	$\frac{2000669}{80640}$	$\frac{516049829}{71280}$	$\frac{26824927062749}{39916800}$
$M_{11,7}(q)$	$\frac{1303}{256}$	$\frac{15734927}{20736}$	$\frac{853191289}{20736}$
$M_{11,8}(q)$	$\frac{3263}{20736}$	$\frac{144101}{20736}$	$\frac{321073}{2304}$
$M_{11,9}(q)$	$\frac{3}{6400}$	$\frac{979}{259200}$	$\frac{9953}{518400}$
$M_{11,10}(q)$	$\frac{1}{39916800}$	$\frac{1}{39916800}$	$\frac{1}{39916800}$
$M_{12,1}(q)$	$\frac{1}{479001600}$	$\frac{1}{479001600}$	$\frac{1}{479001600}$
$M_{12,2}(q)$	$\frac{3}{25600}$	$\frac{979}{777600}$	$\frac{9953}{1244160}$
$M_{12,3}(q)$	$\frac{22841}{248832}$	$\frac{1873313}{248832}$	$\frac{2247511}{9216}$
$M_{12,4}(q)$	$\frac{6515}{1024}$	$\frac{78674635}{31104}$	$\frac{72521259565}{248832}$
$M_{12,5}(q)$	$\frac{1274653}{15360}$	$\frac{98854149649}{1244160}$	$\frac{122245516463717}{6220800}$
$M_{12,6}(q)$	$\frac{2000669}{15360}$	$\frac{46960534439}{213840}$	$\frac{348724051815737}{4561920}$
$M_{12,7}(q)$	$\frac{1274653}{15360}$	$\frac{98854149649}{1244160}$	$\frac{122245516463717}{6220800}$
$M_{12,8}(q)$	$\frac{6515}{1024}$	$\frac{78674635}{31104}$	$\frac{72521259565}{248832}$
$M_{12,9}(q)$	$\frac{22841}{248832}$	$\frac{1873313}{248832}$	$\frac{2247511}{9216}$
$M_{12,10}(q)$	$\frac{3}{25600}$	$\frac{979}{777600}$	$\frac{9953}{1244160}$
$M_{12,11}(q)$	$\frac{1}{479001600}$	$\frac{1}{479001600}$	$\frac{1}{479001600}$

A.3 Program for Evaluation of $P_{n,k}(q)$

```
with(combinat):
 #Poincare polynomial of the moduli space of stable
 #configurations of N points in P^(k-1).
 Poinc:=proc(N,k)
 local A,B,ck,Ck, cN, CN,GS, SN, Sk,i,j, m,n, p,mult, pm, P, S,t;
 #global k1,beta;
 #tau:=0:chi:=0:
 #Use the symmetry P(N,k)=P(N,N-k) to reduce
 #the calculations
 k1:=min(k,N-k);
 n:=N-k1:
 #recursion for Stirling polynomials
 GS[0][0]:=1:
 for i from 1 to n do
       GS[i][1]:=1:GS[i][0]:=0:
 od:
 for i from 1 to k1 do
       GS[-1][i]:=0
 od:
 for i from 0 to n do
       for j from 1 to k1 do
       GS[i][j]:=expand(GS[i][j-1]+GS[i-1][j]*normal((1-q^j)/(1-q)))
       od:
od:
 #changing Stirling polynomials to F-polynomials
 for i from 1 to n do
      for j from k1 to 1 by -1 do
      GS[i][j]:=sum('(-1)^(j-s)*binomial(i+j,i+s)*GS[i][s]','s'=1..j)
      od:
od:
 pm:=-1: P:=0:
 for m from 1 to k1 do
     pm:=-pm:
 #Fixing vertical steps of a path under diagonal.
 #For large k it would be better to count compositions
```

```
#one by one instead of  creating a table!
    Ck:=composition(k1,m):
#the path closest to diagonal with given vertical
#steps ck
     for ck in Ck do
         for i from 0 to m do
#            A[i]:=i;A[m]:=n;
             A[i]:=ceil(sum('ck[s]','s'=1..i)*n/k1);
              B[i]:=n-A[i];
         od;
#we have to count the closest  path  separately
                S:=sum('B[i]*ck[i]', 'i'=1..m-1);
                t:=1:
                for i from 1 to m-1 do
                  if n-B[i]=sum('ck[s]','s'=1..i)*n/k1 then t:=t+1 fi:
                od:
mult:=pm*factorial(N)*(1/t)/product(factorial(B[s-1]-B[s]+ck[s]),s=1..m);
                P:=P+expand(product(GS[B[s-1]-B[s]][ck[s]],
s=1..m)*q^S)*mult;
#S1:=S+sum('ck[i]*(ck[i]-1)/2','i'=1..m);
#tau:=tau+(-1)^S1*pm*mult;
#chi:=chi+1;
#the next path in lexicographic order
         while B[1]>m-1 do
                for i from m-1  by -1 to 1 do
                      if B[i]>m-i then
                             for j from m-1 by -1 to i do
                                   B[j]:=min(B[i]-1+i-j,n-A[j])
                             od;
                             break
                      fi;
                od;
                S:=sum('B[i]*ck[i]', 'i'=1..m-1);
                 t:=1;
                for i from 1 to m-1 do
                  if n-B[i]=sum('ck[s]','s'=1..i)*n/k1 then t:=t+1:fi:
                od:
mult:=pm*factorial(N)*(1/t)/product(factorial(B[s-1]-B[s]+ck[s]),s=1..m);
```

```
                P:=P+expand(product(GS[B[s-1]-B[s]][ck[s]],
s=1..m)*q^S)*mult;
          od:
     od:
 od:
P:=sort(normal(P/(q-1)^(k1-1)));
 RETURN(P);
 end;
```

Bibliography

[T-V] M. A. Tsfasman, S. G. Vladuts, *Algebraic Geometric Codes*, Kluwer Academic Publishers, Dortrecht, Boston, London, 1991.

[Mum] D. Mumford, *Geometric Invariant Theory*, Springer, 1965.

[Gon] A. A. Goncharov, *Geometry of configurations, poylogarithms and motivic cohomology*, Adv. in Math. 114 (1995), 197-318.

[Kly1] A. A. Klyachko, *Betti numbers of space of Hermitian operators of given spectra and sum.*, Preprint LITP 94.43, Univ. Paris VI-VII (1994), 19p.

[Kly2] A. A. Klyachko *Cohomology of Stable Configurations and Mass Formula for Codes.* Preprint.

[Kly3] Meeting Notes with Professor Alexander A. Klyachko.

[Sha] Shannon, C. E. A Mathematical Theory of Communication. *BellSyst. Tech. J.*, 27, pp. 379-423, 623-656 (1948).

[Del] P. Deligne, La Conjecture de Weil. I., *Inst. Hautes Études Sci. Publ. Math. No. 43* (1974), 273-307.

[Wei] A. Weil, *Bull. Amer. Math. Soc. 55* (1949) 497-508; MR 10, 592.